CA Network Flow Analysis

Manuel de l'administrateur

Version 9.3.0



Produits référencés CA Technologies

Ce document fait référence aux produits CA Technologies suivants :

- CA Infrastructure Management
- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Performance Center
- CA ReporterAnalyzer
- CA Single Sign-On

Documentation connexe

CA fournit une documentation technique complète dans la bibliothèque de CA Network Flow Analysis. Accédez à la bibliothèque en cliquant sur le lien Aide dans l'interface utilisateur de CA Network Flow Analysis. Les fichiers PDF et HTML des manuels sont disponibles dans la bibliothèque de la documentation.

La documentation a peut-être été mise à jour depuis sa publication. Pour connaître les dernières mises à jour de la documentation CA Network Flow Analysis et obtenir les versions localisées de la documentation, téléchargez la bibliothèque à partir du site de support CA.

La documentation de CA Network Flow Analysis 9.3.0 inclut les manuels suivants :

- *Aide en ligne* : assistance destinée aux administrateurs et opérateurs, disponible à partir du lien Aide dans l'interface utilisateur
- *Manuel de l'administrateur* : procédure de configuration et de maintenance de CA Network Flow Analysis
- *Manuel de l'opérateur* : procédure d'utilisation de la console NFA pour la création, l'affichage et la gestion des rapports
- *Manuel d'installation* : procédure d'installation du logiciel et de réalisation des tâches de configuration à usage unique
- *Manuel de mise à niveau* : procédure de mise à niveau du logiciel et de réalisation des tâches initiales de configuration
- *Notes de parution* : récapitulatif des améliorations apportées à CA Network Flow Analysis, des corrections et des problèmes en cours de résolution
- *Manuel de CA Anomaly Detector* : procédure d'installation, de mise à niveau, de configuration et d'utilisation de CA Anomaly Detector
- *Notes de parution de CA Anomaly Detector* : présentation du produit, configuration/recommandations système requises et fonctionnalités

Les PDF du produit se trouvent dans le répertoire suivant : <chemin_installation>\Reporter\NetQoS.ReporterAnalyzer.WebSite\help\fr_FR\NFA_Bookshelf\Bookshelf_Files\PDF.

Adobe Reader doit être installé pour pouvoir afficher les fichiers de documentation au format PDF.

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 1: Introduction

Ce chapitre traite des sujets suivants :

CA Network Flow Analysis

CA Network Flow Analysis fournit une analyse du trafic réseau avec une visibilité en temps réel du trafic dans l'ensemble de votre entreprise. Vous pouvez accéder aux données de flux remontant à 1 an maximum pour l'ensemble de votre réseau.

CA Network Flow Analysis est conçu pour être intégré comme une source de données dans le programme utilisé par votre entreprise, qu'il s'agisse de CA Performance Center ou de CA NetQoS Performance Center. La console Performance Center affiche les données de rapport provenant de CA Network Flow Analysis et de tout autre programme intégré comme une source de données.

Ce manuel décrit les tâches d'administration possibles dans la console NFA. D'autres tâches d'administration sont disponibles dans la console Performance Center : gestion des utilisateurs, des rôles, des autorisations, des profils SNMP et de plusieurs types de groupes.

Installez Performance Center et enregistrez CA Network Flow Analysis comme source de données pour pouvoir utiliser toutes les fonctionnalités. Vous pouvez accéder à Performance Center à partir de la console NFA, dès l'enregistrement du produit.

Remarque : Dans ce manuel, le terme *Performance Center* fait collectivement référence à CA Performance Center et à CA NetQoS Performance Center. Les noms de page ou les fonctions spécifiques du programme peuvent être identifiés à l'aide du nom complet ou de l'acronyme du programme, c'est-à-dire *CA PC* pour CA Performance Center et *NPC* pour CA NetQoS Performance Center.

Avis relatifs aux tiers et contrats de licence

Des logiciels tiers sont intégrés dans CA Network Flow Analysis. Tous les logiciels tiers ont été utilisés en accord avec les termes et conditions pour l'utilisation, la reproduction et la distribution, tels que définis par les contrats de licence applicables.

Les informations concernant les contrats de licence tiers sont fournies dans le document suivant, installé automatiquement avec le logiciel :

<chemin_installation>\ThirdPartyContent\ThirdPartyLicenseInfo.pdf

Chapitre 2: Configuration initiale

Une fois le logiciel CA Network Flow Analysis installé, des opérations supplémentaires de configuration sont requises. Les rubriques suivantes contiennent les informations qui vous permettront de configurer CA Network Flow Analysis initialement.

Ce chapitre traite des sujets suivants :

Authentification unique

L'outil Authentification unique vous authentifie lors du démarrage pour que vous puissiez vous connecter une fois et utiliser plusieurs produits liés sans devoir vous reconnecter à chaque fois. Si vous vous connectez à CA Performance Center, par exemple, vous pouvez accéder aux informations de CA Network Flow Analysis sans devoir vous connecter à nouveau.

Authentification unique est installé automatiquement lorsque vous installez CA Network Flow Analysis.

Remarques :

- L'outil Authentification unique utilise le protocole LDAP (Lightweight Directory Access Protocol), si celui-ci est configuré. L'outil Authentification unique n'utilise pas le protocole LDAP par défaut.
- Pour plus d'informations sur la configuration de l'outil Authentification unique dans le cadre de l'authentification LDAP et pour bénéficier d'autres options, consultez le *Manuel de l'utilisateur de l'authentification unique*, disponible dans la Bibliothèque CA Network Flow Analysis et à partir du site de support en ligne de CA.

Configuration du produit pour une utilisation avec Performance Center

Pour pouvoir effectuer certaines tâches d'administration essentielles, vous devez enregistrer CA Network Flow Analysis au niveau de Performance Center (CA Performance Center ou CA NetQoS Performance Center). Une fois le produit enregistré et les tâches d'administration terminées, les opérateurs peuvent afficher des rapports pertinents dans la console NFA et dans la console Performance Center.

Pour configurer CA Network Flow Analysis, vous devez effectuer les tâches suivantes :

- Enregistrez le produit en tant que source de données dans Performance Center.
- Configurez les éléments suivants dans la console Performance Center :
  - Profils SNMP
  - (Facultatif) Domaines IP
  - Comptes d'utilisateurs, autorisations et rôles
  - (Recommandé) Groupes
- Configurez la collecte de flux.
  - Ajoutez des Harvesters.
  - (concerne uniquement les architectures à trois niveaux distribués) Ajoutez des DSA.
  - Activez les routeurs et les interfaces pour l'exportation des flux.
- (Facultatif) Configurer les interruptions
- (Facultatif) Vérifiez que CA Network Flow Analysis reçoit des données.

Ces tâches sont décrites dans les sections suivantes.

Cette section comprend les rubriques suivantes :

Enregistrement de CA Network Flow Analysis

Enregistrez le produit dans la console Performance Center, sur la page Gérer les sources de données (dans CA PC) ou la page Data Source List (Liste des sources de données, dans NPC).

Remarque : Pour plus d'informations sur le nombre de sources de données que vous pouvez utiliser, consultez les *Notes de parution* de votre version de CA Performance Center.

Procédez comme suit :

1. Vérifiez que vous êtes le seul utilisateur à avoir ouvert une session CA Network Flow Analysis. Si plusieurs utilisateurs effectuent simultanément des opérations d'écriture dans la base de données, des problèmes peuvent survenir.
2. Connectez-vous à la console Performance Center en tant qu'utilisateur possédant le rôle Administrateur.
3. Cliquez sur Administration, Sources de données.

   La liste actuelle des sources de données enregistrées s'affiche sur la page Gérer les sources de données (dans CA PC) ou la page Data Source List (Liste des sources de données, dans NPC).
4. Cliquez sur Ajouter (CA PC) ou New (Nouveau) (NPC).

   La boîte de dialogue Ajouter une source de données s'ouvre.
5. Sélectionnez le type de source de données que vous voulez ajouter dans la liste Type de source.

   Remarque : Tous les produits CA qui peuvent être enregistrés en tant que sources de données sont affichés dans la liste Type de source. La liste n'est pas filtrée afin de masquer les produits déjà installés.
6. Saisissez le nom d'hôte de la source de données.

   Le nom d'hôte correspond à l'adresse IP ou au nom d'hôte DNS du serveur sur lequel la base de données de cette source de données est installée. En cas de déploiement distribué du produit, fournissez le nom d'hôte de la console NFA ou du serveur autonome.
7. Indiquez le port à utiliser pour contacter CA Network Flow Analysis.

   Pour plus d'informations sur le paramètre de port, consultez le *Manuel de l'utilisateur de CA Single Sign-On*.

8. Sélectionnez le protocole à utiliser pour contacter la source de données. Sélectionnez **https** si votre réseau utilise le protocole SSL pour les communications. Vérifiez que vous avez configuré le système correctement avant de sélectionner l'option **https.**

   Remarque : Pour plus d'informations sur l'utilisation du langage SSL pour la communication entre le produit et Performance Center, reportez-vous au *Manuel de l'utilisateur de CA Single Sign-On.*

9. (Facultatif) Saisissez un nom d'affichage pour la source de données CA Network Flow Analysis.

   Si vous ne spécifiez pas de nom, un nom par défaut est créé en combinant le type de source de données et le nom d'hôte. Par exemple, vous pouvez utiliser un nom par défaut comme NetworkFlowAnalysis@xxx.x.x.xx ou vous pouvez utiliser un nom de type NetworkFlowAnalysis_NewYork.

10. Confirmez si l'adresse de console Web est identique au nom de l'hôte. Si ce n'est pas le cas, procédez comme suit :

    - Désélectionnez la case à cocher Mêmes éléments que la source de données.
    - Fournissez le nom d'hôte de console Web, le port et le protocole.

11. Cliquez sur Enregistrer.

    La liste mise à jour indique les sources de données qui sont enregistrées.

Test des connexions à la source de données

Dans la plupart des cas, le statut indique que l'enregistrement de source de données est terminé. Si le statut indique une erreur, utilisez la fonctionnalité de test de la page Gérer les sources de données (CA PC) ou Data Source List (Liste des sources de données) (NPC).

Le bouton Test lance un test pour confirmer qu'une nouvelle source de données est enregistrée et connectée correctement. Le test recherche la compatibilité des versions et vérifie que la source de données n'est pas enregistrée auprès d'une instance différente du logiciel.

Si le test échoue, vérifiez que le nom d'hôte DNS ou l'adresse IP du serveur de source de données est correct.

Vérification des profils SNMP

CA Network Flow Analysis envoie des informations SNMP sécurisées à CA Performance Center lors de l'enregistrement. Ces informations sont ensuite transformées en profils SNMP. *Les profils SNMP* sont des définitions qui contiennent les informations nécessaires pour activer des requêtes sécurisées de MIB d'unité à l'aide de SNMP. Les informations de profil sont mises à jour à chaque synchronisation (toutes les cinq minutes).

Lors de l'installation initiale du produit, vérifiez que les profils SNMP disponibles sont adéquats pour surveiller votre environnement. Les profils SNMP disponibles sont répertoriés dans la page Gérer les profils SNMP (CA PC) ou SNMP Profile List (Liste de profils SNMP) (NPC).

Affichage de la liste de profils SNMP

Vous pouvez afficher la liste des profils SNMP qui ont déjà été définis. La liste inclut des informations de haut niveau concernant le contenu de chaque profil.

Profils spécifiques de client hébergé dans CA Performance Center :

- Si aucune définition de client hébergé n'a été créée, les définitions de la liste de profils SNMP sont partagées entre toutes les sources de données enregistrées. L'administrateur global peut afficher une liste des profils SNMP qui ne sont pas associés explicitement à un client hébergé.
- Les administrateurs de clients hébergés voient uniquement les éléments associés à leur client hébergé.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur avec le rôle Administrateur.
2. Affichez la liste des profils SNMP :
   - CA PC : sélectionnez Administration, Paramètres du système : Profils SNMP.
   - NPC : sélectionnez Admin (Administration), NetQoS Settings (Paramètres NetQoS) : SNMP Profiles (Profils SNMP).

   Elle affiche la liste actuelle des profils SNMP.

   Les informations suivantes sont répertoriées pour chaque profil :

   Classer

   Détermine l'ordre dans lequel les informations sécurisées contenues dans un profil SNMP sont utilisées pour essayer d'interroger une unité sélectionnée. Si la requête échoue, le profil suivant est utilisé, dans l'ordre de priorité.

Nom du profil

Définit le nom du profil SNMP. Les noms de profil doivent être uniques, ne peuvent pas être dupliqués sur les différentes versions SNMP et ne sont pas sensibles à la casse.

Port (CA PC uniquement)

Identifie le port utilisé pour établir des connexions SNMP avec les unités.

Valeur par défaut : UDP 161.

Version SNMP

Spécifie la version de SNMP que le profil utilise. Dans la mesure où SNMPv1 et SNMPv2C sont similaires du point de vue de la sécurité, ils partagent une option unique. SNMPv3 est une option distincte.

Protocole d'authentification

(SNMPv3 uniquement) Spécifie le protocole d'authentification à utiliser pour contacter des unités associées à ce profil. Les algorithmes d'authentification des paquets SNMPv3 suivants sont pris en charge :

- Aucun (n'essayez pas l'authentification)
- MD5 (Résumé de message 5)
- SHA (Algorithme de hachage sécurisé)

Protocole de confidentialité

Identifie le protocole de chiffrement utilisé pour contacter les unités associées, le cas échéant. Toujours Aucun si aucun protocole d'autorisation n'est en cours d'utilisation.

Utiliser par défaut

Indique si les informations figurant dans ce profil sont utilisées lorsqu'il n'est pas explicitement affecté à une unité. S'il est désactivé, ce profil est exclu de la détection dans les sources de données qui prennent en charge l'exclusion de profils.

Pour effectuer une action dans cette page, sélectionnez un profil, puis cliquez sur un bouton.

Ajout des profils SNMP

Les administrateurs peuvent créer des profils SNMP dans la console CA Performance Center. Vous pouvez créer des profils SNMPv1/v2C ou SNMPv3.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur possédant le rôle Administrateur.
2. Affichez la liste des profils SNMP :
   - CA PC : sélectionnez Administration, Paramètres du système : Profils SNMP.
   - NPC : sélectionnez Admin (Administration), NetQoS Settings (Paramètres NetQoS) : SNMP Profiles (Profils SNMP).

   Elle affiche la liste actuelle des profils SNMP.
3. Cliquez sur Créer.

   La boîte de dialogue Ajouter un profil SNMP s'affiche.
4. Remplissez les champs et modifiez les paramètres par défaut nécessaires. Certains champs s'appliquent uniquement au profil SNMPv3 ou SNMPv.1/v2C

   Nom du profil

   Définit le nom du profil SNMP. Les noms de profil doivent être uniques, ne peuvent pas être dupliqués sur les différentes versions SNMP et ne sont pas sensibles à la casse.

   Version SNMP

   Spécifie la version de SNMP que le profil utilise. Dans la mesure où SNMPv1 et SNMPv2C sont similaires du point de vue de la sécurité, ils partagent une option unique. SNMPv3 est une option distincte.

   Port

   (Facultatif pour SNMPv1/v2C) Identifie le port utilisé pour réaliser les connexions SNMP avec les unités associées à ce profil.

   Valeur par défaut : UDP 161.

   User Name

   (SNMPv3 uniquement) Identifie l'utilisateur pour le profil, dont les clés secrètes ont été utilisées pour authentifier et chiffrer les paquets SNMPv3. Le nom d'utilisateur est une chaîne de caractères.

   Nom du contexte

   (SNMPv3 uniquement) Spécifie une collection d'informations de gestion accessible par une entité SNMP. Le nom de contexte est nécessaire pour fournir une identification bout en bout et pour la récupération des données à partir d'un agent SNMPv3. Le nom de contexte est une chaîne d'octets.

Nom de communauté

(SNMPv1/v2C seulement) Définit une chaîne sécurisée qui permet à la source de données d'interroger la MIB de l'unité associée. La communauté que vous spécifiez doit fournir un accès en lecture seule à la MIB de l'unité.

Remarque : Dans le profil SNMP par défaut, la communauté est "public".

Vérifier le nom de la communauté

Confirme la chaîne de communauté sécurisée (nom).

Protocole d'authentification

(SNMPv3 uniquement) Spécifie le protocole d'authentification à utiliser pour contacter des unités associées à ce profil. Les algorithmes d'authentification des paquets SNMPv3 suivants sont pris en charge :

- Aucun (n'essayez pas l'authentification)
- MD5 (Résumé de message 5)
- SHA (Algorithme de hachage sécurisé)

Mot de passe d'authentification

(SNMPv3 uniquement) Spécifie le mot de passe pour l'authentification à l'aide de SNMPv3 et du protocole d'authentification sélectionné.

Remarque : Pour les profils SNMP utilisés avec CA Network Flow Analysis, assurez-vous que le mot de passe spécifié comprend huit caractères au minimum. Si le mot de passe ne répond pas à cette exigence, le profil SNMP n'est pas valide et aucune donnée SNMP ne sera renvoyée lorsque le profil SNMP est utilisé pour l'interrogation. Dans ce cas, les noms d'unités, les noms d'interfaces, les vitesses d'interfaces et les données d'utilisation des interfaces sont manquantes pour les interfaces et les unités correspondantes dans les vues, les rapports et les tableaux de bord.

Vérifier le mot de passe d'authentification

Confirme le mot de passe d'authentification.

Protocole de confidentialité

(Facultatif) Spécifie le protocole de chiffrement à utiliser pour des flux de données envoyés aux unités ou aux serveurs associés à ce profil. Pour créer un profil SNMP valide pour l'interrogation CA Network Flow Analysis, sélectionnez l'un des protocoles suivants :

- Aucun (ne pas chiffrer les communications)
- DES
- AES (chiffrement 128 bits)
- Triple DES

Remarque : Si les options AES 192 et AES 256 sont répertoriées, ne les sélectionnez pas, car elles ne sont pas prises en charge pour CA Network Flow Analysis. Si le profil SNMP que vous créez n'est pas valide, aucune donnée SNMP n'est renvoyée pour les unités et les interfaces qui l'utilisent. Dans ce cas, les noms d'unités, les noms d'interfaces, les vitesses d'interfaces et les données d'utilisation des interfaces sont manquantes pour les interfaces et les unités correspondantes dans les vues, les rapports et les tableaux de bord.

L'option de protocole de confidentialité est activée uniquement si l'authentification est activée pour ce profil.

Mot de passe de confidentialité

Définit le mot de passe utilisé lors de l'échange des clés de chiffrement. Consultez la remarque pour connaître les configurations de longueurs possibles.

Vérifier le mot de passe de confidentialité

Définit le mot de passe utilisé lors de l'échange des clés de chiffrement.

Use by default for new devices (Utiliser ce port par défaut pour les nouvelles unités) (CA PC)

Enable this profile for auto-discovery (Activer ce profil pour la détection automatique) (NPC)

Spécifie si le profil est utilisé par défaut pour contacter toute nouvelle unité qui est détectée à partir du trafic surveillé. S'il échoue, le profil suivant dans l'ordre de priorité est utilisé. Désactivez ce paramètre pour exclure un profil de la détection.

5. Cliquez sur Enregistrer.
6. Vous retournez à la liste de profils SNMP. Le nouveau profil apparaît dans la liste.

   CA Performance Center effectue une synchronisation globale pour envoyer les informations de profil à CA Network Flow Analysis.

Vérification des domaines IP

La fonctionnalité de domaines IP permet de résoudre les conflits d'adresse IP potentiels. Les identificateurs de domaine indiquent que deux éléments gérés qui apparaissent par ailleurs en tant qu'adresses IP en double sont en fait deux éléments gérés *différents*.

Les domaines IP permettent également aux administrateurs globaux de CA Performance Center de contrôler les éléments gérés que les différents administrateurs ou utilisateurs peuvent visualiser ou auxquels ils peuvent accéder.

Les informations concernant les domaines IP personnalisés sont transmises aux sources de données pendant la synchronisation. Les domaines sont disponibles pour l'utilisation pendant la configuration. Vous pouvez utiliser les fonctions d'administration de la console NFA pour ajouter des interfaces, des interfaces virtuelles personnalisées, des routeurs et des Harvesters aux domaines personnalisés que vous créez.

Lors de l'installation initiale, vérifiez que les domaines IP disponibles sont appropriés à la surveillance de votre environnement. Pour afficher les domaines, effectuez l'une des opérations suivantes dans la console CA Performance Center :

- (CA PC) Sélectionnez Administration, Domaines IP et vérifiez les domaines dans la page Gérer les domaines IP.
- (NPC) Sélectionnez Admin (Administration), Groups (Groupes) et développez l'arborescence All Groups (Tous les groupes) dans la page Manage Groups (Gérer les groupes).

Affichage de la liste de domaines IP

Les domaines IP sont requis pour surveiller plusieurs environnements dont les adresses IP se chevauchent. Configurez tous les domaines dont vous avez besoin avant de commencer à exporter les données de flux.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle administratifs requis.
2. Affichez les domaines actuels en effectuant l'une des actions suivantes :
   - (CA PC) Sélectionnez Administration, Paramètres du système : Domaines IP.

     La page Gérer les domaines IP s'ouvre et affiche les domaines actuels.
   - (NPC) Sélectionnez Admin (Administration), NetQoS Settings: Groups (Paramètres NetQoS : Groupes) et développez l'arborescence All Groups (Tous les groupes) dans la page Manage Groups (Gérer les groupes).

     Les domaines actuels sont affichés sous l'arborescence All Domains (Tous les domaines). Pour afficher les paramètres d'un domaine dans CA NetQoS Performance Center, sélectionnez le domaine et cliquez sur l'onglet Properties (Propriétés).

Si vous n'avez pas créé de domaines IP personnalisés, seul le domaine par défaut s'affiche dans la liste. Ce domaine prédéfini présente le paramètre Nul pour tous les paramètres.

Tous les domaines personnalisés que vous avez créés comprennent des valeurs pour les paramètres suivants :

Nom

Identifie le domaine.

Description

(Facultatif) Décrit cet espace de noms de domaine, par exemple en nommant l'entreprise qui le possède.

Adresse du DNS principal

Adresse IP du serveur de noms principal pour ce domaine.

Port DNS principal

Numéro de port utilisé par le serveur de noms principal

Adresse DNS secondaire

Adresse IP du serveur de noms secondaire pour ce domaine. Peut être la même que l'adresse principale.

Port DNS secondaire

Numéro de port utilisé par le serveur de noms secondaire.

Ajout de domaines IP personnalisés

Les administrateurs peuvent définir l'affectation de domaine pour des Harvesters, des routeurs, des interfaces et des interfaces virtuelles personnalisées. Il est recommandé de configurer chaque client hébergé et domaine personnalisé nécessaire avant d'ajouter des Harvesters.

La configuration des domaines IP appropriés facilite la réalisation des objectifs suivants :

- Affectation du client hébergé et du domaine corrects lors de l'ajout de Harvesters, de sorte que leurs routeurs et leurs interfaces héritent des associations correctes. Les routeurs disposent des profils SNMP appropriés disponibles pour interroger leurs interfaces.
- Mise à disposition du contenu spécifique uniquement pour les opérateurs qui doivent le surveiller
- Administrateurs autorisés à créer des étiquettes de type de service propres au domaine, aux groupes de protocoles et aux noms de systèmes autonomes dans CA Network Flow Analysis
- Conflits d'adresses IP évités.

  Supposons qu'un routeur disposant d'une adresse IP unique contienne des interfaces appartenant à différentes entreprises. Les identificateurs de domaine indiquent que les interfaces constituent des éléments gérés différents, même si l'adresse IP est identique.

Le domaine par défaut est créé automatiquement. Le domaine par défaut inclut tous les éléments qui ne sont pas affectés à un domaine personnalisé.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle administratifs requis.
2. Affichez les domaines actuels en effectuant l'une des actions suivantes :
   - (CA PC) Sélectionnez Paramètres du système : Domaines IP.

     La page Gérer les domaines IP s'ouvre et affiche les domaines actuels.
   - (NPC) Sélectionnez Admin, NetQoS Settings: Groups (Paramètres NetQoS : Groupes) et développez l'arborescence All Groups (Tous les groupes) de la page Manage Groups (Gérer les groupes).

     Les domaines actuels sont affichés sous l'arborescence All Domains (Tous les domaines).

   Si vous n'avez pas créé de domaines IP personnalisés, seul le domaine par défaut s'affiche dans la liste.
3. Créez un nouveau domaine :
   - (CA PC) Cliquez sur Créer.

     La boîte de dialogue Administration des domaines IP s'ouvre.
   - (NPC) Cliquez avec le bouton droit de la souris sur All Domains (Tous les domaines) et sélectionnez Add New Domain (Ajouter un nouveau domaine).

     La boîte de dialogue Add Domain (Ajouter un domaine) s'affiche.
4. Fournissez des informations pour les paramètres suivants :

   Domaine Nom

   Identifie le domaine.

   Description

   (Facultatif) Décrit cet espace de noms de domaine, par exemple en nommant l'entreprise qui le possède.

   Alias de l'unité

   (CA PC uniquement) Indique l'alias à utiliser pour une unité gérée. Un alias d'unité est un nom configuré par l'utilisateur appliqué à l'élément géré associé dans CA Performance Center. Cliquez sur Parcourir pour rechercher un fichier CSV d'alias et l'importer. Le fichier CSV contient une liste de mappages d'adresses vers les alias d'unités IP séparés par une virgule.

   Les alias associés à l'adresse IP principale d'une unité sont prioritaires sur les alias associés aux adresses IP secondaires. Recherchez l'adresse IP principale dans la colonne Adresse de la liste Inventaire - Unités. Nous vous recommandons de toujours utiliser l'adresse IP principale de l'unité dans le fichier CSV.

Par exemple :
`172.24.36.107, routeur Austin`

Sélectionnez le fichier, puis cliquez sur Ouvrir.

Si vous incluez des alias pour des unités que vous gérez déjà, un délai de 5 minutes peut être requis avant le début de la synchronisation de ces alias avec CA Performance Center.

Remarque : Pour supprimer un alias, importez un fichier CSV qui inclut l'adresse IP de l'unité et une colonne d'alias vide. Pour changer un alias, modifiez l'entrée de l'alias dans le fichier CSV et réimportez le fichier.

Substitution de description d'interface

(CA PC uniquement) Indique une autre description à utiliser pour une interface. Des descriptions d'interface apparaissent déjà dans CA Performance Center, mais vous pouvez fournir une autre description. Cliquez sur Parcourir pour rechercher un fichier CSV ou TXT contenant d'autres descriptions et l'importer. Le fichier contient une liste de valeurs séparées par des virgules qui incluent les mappages d'adresse IP d'unité, de nom d'interface, de description d'interface et d'autres descriptions d'interfaces (alias).

Par exemple :
`172.24.36.107,ethernet_7,vmxnet3 Ethernet Adapter,connexion à Dallas`

Remarque : Utilisez l'adresse IP principale de l'unité associée dans le fichier CSV ou TXT. Les adresses IP secondaires ne sont pas prises en charge. Recherchez l'adresse IP principale dans la colonne Adresse de la liste Inventaire - Unités.

Sélectionnez le fichier, puis cliquez sur Ouvrir.

Si vous incluez d'autres descriptions pour des interfaces que vous gérez déjà, un délai de 5 minutes peut être requis avant le début de la synchronisation de ces descriptions avec CA Performance Center.

Remarque : Vous pouvez utiliser les descriptions d'interface alternatives pour plusieurs interfaces.

Pour supprimer une description alternative, importez un fichier CSV ou TXT qui inclut l'adresse IP de l'unité, le nom d'interface, la description d'interface et une colonne d'alias vide. Lorsque vous supprimez une description alternative, la description d'origine de l'interface est restaurée dans les vues de CA Performance Center.

Important : Si vous utilisez un programme de tableur pour supprimer toutes les descriptions alternatives d'un fichier CSV, incluez un en-tête pour la colonne de substitution de description d'interface dans le fichier importé. Si vous n'incluez pas cet en-tête de colonne, les descriptions d'interface d'origine ne s'afficheront plus dans les vues de CA Performance Center.

Pour changer une description, modifiez l'entrée de l'alias dans le fichier CSV ou TXT et réimportez le fichier.

Case à cocher Paramètres de DNS

(CA PC uniquement) Si cette option est sélectionnée, les options Port DNS principal et Port DNS secondaire sont affichées.

Adresse du DNS principal

Adresse IP du serveur de noms principal pour ce domaine.

Port DNS principal

Numéro de port utilisé par le serveur de noms principal

Adresse DNS secondaire

Adresse IP du serveur de noms secondaire pour ce domaine. Peut être la même que l'adresse principale.

Port DNS secondaire

Numéro de port utilisé par le serveur de noms secondaire.

Activer l'adresse de proxy DNS

(NPC uniquement) Indique si l'adresse du proxy est activée pour ce domaine IP.

Adresse de proxy DNS

(NPC uniquement) Adresse IP du serveur proxy DNS.

Ce paramètre est requis uniquement si votre réseau se trouve derrière un serveur proxy DNS.

5. Cliquez sur Enregistrer.

   Le nouveau domaine IP apparaît sur la page.

6. Répétez les étapes comme requis pour ajouter d'autres domaines IP.

Configuration de la collecte de flux

L'étape suivante consiste à configurer les routeurs dans CA Network Flow Analysis et à vérifier qu'ils envoient des données aux composants de collecte.

CA Network Flow Analysis peut commencer à collecter les flux une fois les tâches suivantes terminées :

- Recommandation : Ajoutez les domaines dont vous avez besoin (page 24).
- Ajoutez les Harvesters (page 28).
- (Uniquement pour les architectures distribuées à trois niveaux) Ajoutez des DSA (page 33).
- Configurez les routeurs et les interfaces de façon à ce qu'ils puissent exporter des données de flux (page 31).

Ajout d'un ou de plusieurs Harvesters

Ajoutez un ou plusieurs Harvesters pour permettre le traitement et l'affichage des données.

Condition préalable :

Recommandation : Si ce n'est pas déjà fait, enregistrez CA Network Flow Analysis et configurez des domaines avant d'ajouter un Harvester.

Procédez comme suit :

1. Ouvrez la console NFA et connectez-vous avec des droits d'administrateur. Vous pouvez, par exemple, entrer l'adresse suivante dans un navigateur :

   http://<adresse_IP>/ra/

   Nom d'utilisateur : *admin*

   Mot de passe : *admin*

2. Ouvrez la page Composant de collecte.

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Système : composant de collecte.

      La page Composant de collecte s'affiche et indique les composants de collecte actuels.

3. Cliquez sur Ajouter.

   La boîte de dialogue Ajouter un Harvester s'ouvre.

4. Entrez les informations suivantes :

   Adresse IP

   Adresse du serveur de Harvester.

   Description

   Texte identifiant le Harvester et apparaissant dans la table Harvester.

   Domaine

   Combinaison client hébergé parent/domaine parent pour le Harvester et pour tous les routeurs et toutes les interfaces qui commencent à fournir des données au Harvester.

   Toute modification apportée à ce paramètre affectera la combinaison client hébergé/domaine de chaque nouveau routeur qui commence à exporter des données de flux et de chaque nouvelle interface qui commence à générer des flux.

   Dans un environnement d'hébergement multiclient, le client hébergé du Harvester a une influence sur les profils SNMP disponibles qui permettent aux routeurs d'interroger les interfaces.

   Le domaine affecte les opérateurs et les rapports qui ont accès aux données générées par les routeurs et par les interfaces.

   Cette option est visible uniquement dans les environnements qui contiennent plusieurs domaines.

5. Cliquez sur Enregistrer.

   Le nouveau Harvester est ajouté et apparaît dans la liste des Harvesters, dans le cas où le test de connexion pour l'adresse IP a réussi. Si le test de la connexion au service Web échoue, un message d'erreur apparaît.

   Le processus habituel prévoit l'ajout d'un ou de plusieurs Harvesters, puis la configuration des interfaces de routeur en vue de l'exportation des flux vers les Harvesters. Si vous configurez les routeurs pour l'exportation des flux vers le Harvester, la console NFA lance immédiatement la collecte des données à partir du nouveau Harvester. Le domaine des routeurs est alors défini lorsque vous ajoutez le Harvester parent.

Remarque : Vérifiez que les Harvesters que vous ajoutez n'ont pas été supprimés de la page du Harvester. Pour ajouter une instance de Harvester dans CA Network Flow Analysis 9.3.0 après l'avoir supprimée, vous devez réimager le serveur d'installation de Harvester et réinstaller le logiciel de Harvester.

Vérification du domaine du Harvester

Vérifiez que tous les Harvester sont associés au domaine approprié avant de configurer des routeurs pour l'exportation des données de flux. Si ce n'est pas déjà fait, configurez tout client hébergé et domaine personnalisés nécessaire avant de continuer.

Remarque : La fonctionnalité de client hébergé est applicable uniquement aux déploiements qui incluent CA Performance Center. Si votre déploiement utilise CA NetQoS Performance Center, le paramètre de client hébergé est toujours Client hébergé par défaut.

Procédez comme suit :

1. Ouvrez la page Composant de collecte.
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Système : composant de collecte.

      La page Composant de collecte s'affiche et indique les composants de collecte actuels.

2. Dans la ligne du Harvester que vous souhaitez modifier, cliquez sur Modifier.

   La boîte de dialogue Modifier le Harvester s'ouvre.

3. (Facultatif) Modifiez le paramètre Domaine (combinaison client hébergé/domaine) si nécessaire.

   Valeur par défaut : client hébergé par défaut\domaine par défaut.

   Vous pouvez également modifier l'adresse IP et la description.

   Si aucun domaine IP personnalisé n'a été créé, la table Harvester inclut uniquement les colonnes Adresse IP et Description.

4. Lorsque vous avez effectué vos modifications, cliquez sur Enregistrer.

   Vos modifications sont enregistrées.

Configuration des routeurs

Activez NetFlow sur chaque routeur CA Network Flow Analysis en effectuant les étapes décrites dans cette rubrique. Vous pouvez configurer les routeurs pour exporter un des protocoles de flux suivants :

- NetFlow v5, v7, v9 et Sampled NetFlow
- sFlow version 5
- IPFIX, Jflow, cFlow et NetStream conformes aux normes NetFlow v5, v7 ou v9.

Remarques :

- Configurez le flux de chaque source à exporter vers un seul Harvester. Si le flux d'une source est exporté vers plusieurs Harvesters, divers problèmes surviendront. Si tel est le cas, contactez le Support CA pour obtenir de l'aide.
- NetFlow fournit une vue générale des flux de paquets réseau en créant des enregistrements de flux pour tous les paquets. Les données de ces enregistrements de flux représentent tous les paquets. Les protocoles NetFlow/IPFIX et sFlow donnés en exemple extraient des échantillons à partir de vos flux de paquets, afin de réduire le nombre d'enregistrements de flux générés et de diminuer l'impact sur un collecteur. Plus le taux d'échantillonnage est faible, moins précises sont les données.

Pour que les données des flux non échantillonnés apparaissent dans les rapports incluant 15 minutes de données (historique), les champs suivants sont obligatoires :

- L'un des champs suivants : 1 - IN_BYTES, 85 - IN_PERMANENT_BYTES, 231 - FW_INITIATOR_OCTETS ou 232 - FW_RESPONDER_OCTETS
- 4 - PROTOCOL
- 7 - L4_SRC_PORT
- 8 - IPV4_SRC_ADDR
- 10 - INPUT_SNMP
- 11 - L4_DST_PORT
- 12 - IPV4_DST_ADDR
- 14 - OUTPUT_SNMP

Effectuez ces tâches :

1. Sauvegardez la configuration actuelle du routeur.
2. Configurez l'exportation NetFlow pour chaque interface individuellement.
   a. Définissez la version d'exportation du flux.
   b. Définissez l'adresse IP source du flux. Cisco recommande de configurer une interface source de bouclage. Les adresses IP d'interfaces autres que des interfaces de bouclage peuvent changer.
   c. Définissez l'adresse IP de destination du flux et définissez le port de destination sur 9995. Si vous utilisez une valeur personnalisée pour le port d'écoute de l'Harvester, utilisez cette valeur comme port de destination. Les valeurs de port doivent correspondre pour que le Harvester puisse recevoir les données de flux.
   d. Définissez le délai d'expiration du flux sur 1 minute.
3. Activez le flux pour chaque interface.
   - NetFlow v5 ou flux compatible avec v5 :
     - Surveillance de plusieurs interfaces sur un routeur : utilisez toutes les entrées et toutes les sorties. Utilisez la même option pour toutes les interfaces. Les valeurs d'entrée et de sortie peuvent varier légèrement à cause des routeurs qui omettent des paquets et des valeurs de types de services changeantes telles que le trafic entre les interfaces.
     - Surveillance d'une seule interface sur un routeur : utiliser les entrées et les sorties. Avec cette option, moins de flux totaux sont générés du routeur au Harvester et la charge sur le réseau et le Harvester est moins élevée.
   - NetFlow v9 ou flux compatible avec v9 :

     Le Harvester identifie et déduplique plusieurs flux sur un routeur unique, pour vous permettre d'utiliser les entrées et les sorties sur plusieurs interfaces. Cette option peut s'avérer très efficace pour deux ou trois interfaces. Vous pouvez activer les entrées et les sorties pour toutes les interfaces, mais cette configuration peut représenter une charge supplémentaire inutile pour le Harvester.
4. Configurez la persistance de l'index SNMP sur chaque routeur prenant en charge cette fonctionnalité.

Ajout de DSA (déploiement à trois niveaux)

Applicable à : une architecture à trois niveau dans un déploiement distribué (console NFA, Harvester et DSA installés sur des serveurs distincts)

Dans un déploiement d'architecture à trois niveaux, ajoutez un ou plusieurs DSA pour stocker les données de résolution en 15 minutes (historiques). Dans le cas d'un système autonome ou d'une architecture à deux niveaux, n'ajoutez pas de DSA.

Nous vous recommandons d'ajouter au moins un DSA dans les 30 minutes suivant le lancement de la collecte des flux. Pour que les données de résolution en 15 minutes apparaissent dans les rapports, vous devez ajouter un DSA au déploiement à trois niveaux. Les rapports qui affichent une plage horaire supérieure à 2 heures n'affichent aucune donnée.

Remarque : Modifiez l'adresse IP du DSA retiré plutôt que d'ajouter une instance de DSA. Sinon, les routeurs continuent d'envoyer des données au DSA retiré (et ces données n'apparaissent pas dans les rapports). Si vous devez supprimer un DSA, contactez le support CA pour obtenir de l'aide.

Procédez comme suit :

1. Ouvrez la console NFA et connectez-vous avec des droits d'administrateur.
2. Affichez la page DSA dans l'interface utilisateur de la console NFA :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Système : DSA.

      La page DSA s'ouvre et affiche la liste des DSA utilisés.
3. Cliquez sur Ajouter.

   La boîte de dialogue Ajouter un DSA s'affiche.
4. Indique l'adresse IP du serveur de DSA.
5. Cliquez sur Tester la connexion.

   Un test de connexion est effectué pour déterminer si le serveur de la console NFA peut contacter le serveur de DSA et vérifier que MySQL est installé. Si le test réussit, le message suivant apparaît : Test réussi.
6. Répondez au résultat du test :
   a. Si le message Test réussi s'ouvre, cliquez sur OK pour le fermer.
   b. Si un message d'erreur apparaît, fermez le message et suivez la procédure décrite dans la rubrique Dépannage en cas d'ajout de DSA (page 35).

7. Une fois le test terminé, cliquez sur Enregistrer dans la boîte de dialogue Ajouter un DSA.

   Le test de connexion est effectué, suivi d'un test permettant de localiser les paramètres de DSA sur le serveur cible.

8. Notez le résultat du test :

   - L'absence de message d'erreur indique que les tests ont réussi. Les résultats suivants se produisent :
     - La boîte de dialogue se ferme et le DSA est ajouté à la liste de DSA.
     - Les Harvesters incluent le nouveau DSA dans les destinations pour les nouvelles interfaces activées qui signalent des données de résolution en 15 minutes.
     - La console NFA transfère les paramètres vers le nouveau DSA.
     - Le DSA est configuré pour récupérer les fichiers de données de résolution en 15 minutes de la console NFA.
     - Les données du DSA apparaissent dans les rapports dans un délai de 30 minutes.
   - Si un message d'erreur apparaît, fermez le message et suivez la procédure décrite dans la rubrique Dépannage en cas d'ajout de DSA (page 35).

Remarques :

- Si un DSA ne commence pas la collecte des données de résolution en 15 minutes dans un délai de 30 minutes après le début de la collecte des flux, des problèmes peuvent se produire. Les données traitées s'accumulent sur le serveur de la console NFA et le traitement est ralenti. Si le problème persiste, la console NFA ne collecte plus les données de résolution en 15 minutes et les données non traitées s'accumulent sur les Harvesters. Si les interruptions de l'outil de surveillance sont configurées, l'outil envoie des alertes indiquant un retard du Harvester ou du Reaper. Si le problème n'est pas résolu, l'exécution des services CA Network Flow Analysis sur les Harvesters peut s'interrompre.
- Chaque DSA est activé pour collecter des données pour un maximum de 5 000 interfaces activées ayant signalé des données.
- Pour plus d'informations sur les types de données, la durée du stockage, les seuils minimum et les types de rapports pour les données de résolution en 15 minutes stockées sur des serveurs de DSA, consultez la rubrique Données de résolution en 15 minutes (page 193) du *Manuel de l'administrateur de CA Network Flow Analysis*.

Dépannage en cas d'ajout de DSA

Applicable à : une architecture à trois niveau dans un déploiement distribué (console NFA, Harvester et DSA installés sur des serveurs distincts)

Si un des messages d'erreur suivants apparaît lorsque vous cliquez sur Tester la connexion ou sur Enregistrer dans la boîte de dialogue Ajouter un DSA, fermez le message d'erreur et suivez la procédure décrite.

Erreurs de test de connexion

Utilisez les conseils suivants pour corriger les erreurs qui peuvent apparaître lorsque vous cliquez sur Tester la connexion dans la boîte de dialogue Ajouter un DSA.

- L'adresse IP de serveur spécifiée n'est pas valide :

  Vous avez entré un format d'adresse IP non valide. Vérifiez que l'adresse IP entrée est correcte.

- "System.Web.Services.Protocols.SoapException...'":

  Vérifiez que le service NetQoS MySql s'exécute sur le serveur de la console NFA. Si le service n'est pas en cours d'exécution, démarrez-le.

- Unable to connect to any of the specified MySQL hosts (la connexion à un des hôtes MySQL spécifiés est impossible) :

  Démarrez le service NetQoS MySql sur le serveur du DSA. Vérifiez que le service NetQoS MySql s'exécute sur le serveur du DSA. Si le service n'est pas en cours d'exécution, démarrez-le.

- Unknown database nqrptr (base de données nqrptr inconnue) :

  La base de données de DSA nqrptr n'a pas été trouvée sur le serveur cible. Vérifiez que l'installation du logiciel DSA est terminée.

Erreurs d'enregistrement

Utilisez les conseils suivants pour corriger les erreurs qui peuvent apparaître lorsque vous cliquez sur Enregistrer dans la boîte de dialogue Ajouter un DSA.

- Un enregistrement existant est déjà en cours d'utilisation :

  Entrez l'adresse IP d'un DSA qui n'est pas déjà dans la liste de DSA.

- Connection must be valid and open (la connexion doit être valide et ouverte) :

  Vérifiez que le service NetQoS MySql s'exécute sur le serveur du DSA. Si le service n'est pas en cours d'exécution, démarrez-le.

- "System.Web.Services.Protocols.SoapException...'":

  Vérifiez que le serveur cible s'exécute et est accessible par le serveur de la console NFA. Vérifiez que le service NetQoS MySql s'exécute sur le serveur de la console NFA. Si le service n'est pas en cours d'exécution, démarrez-le.

- Table 'nqrptr.settings' doesn't exist (la table nqrptr.settings n'existe pas)

  La table de paramètres de DSA n'a pas été trouvée. Le logiciel de DSA n'a pas été installé correctement sur le serveur cible.

  - Vérifiez que vous avez entré l'adresse IP correcte pour le DSA (et non l'adresse IP d'un Harvester ou de la console NFA).
  - Vérifiez que l'installation du logiciel DSA est terminée.

Vérification de la réception des données

Pour vérifier que les données sont reçues, effectuez les tâches suivantes :

- Vérification de l'activation des interfaces (page 36)
- Vérification de la visibilité des interfaces dans la console NFA (page 37)

Vérification de l'activation des interfaces

Une fois que vous avez configuré CA Network Flow Analysis pour la réception des données de flux, vérifiez que les interfaces surveillées sont celles attendues.

Procédez comme suit :

1. Ouvrez la console NFA et connectez-vous avec des droits d'administrateur.
2. Ouvrez la page Interfaces disponibles :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Système : Activer les interfaces.

      La page Interfaces disponibles s'ouvre.
3. Pour afficher la liste d'interfaces, cliquez sur la flèche à gauche du nom du routeur pour développer les détails du routeur.
4. Examinez la liste pour savoir quelles interfaces sont activées.
5. Pour modifier le statut d'une interface, activez la case à cocher à côté d'une ou de plusieurs interfaces, puis cliquez sur Activer ou Désactiver.

   Les interfaces sélectionnées sont activées ou désactivées.
6. Répétez ces étapes pour chaque routeur.

Vérification de la visibilité des interfaces dans la console NFA

Vérifiez que les interfaces s'affichent dans la console NFA.

1. Vérifiez que les interfaces sont visibles dans la page Présentation d'entreprise :
    a. Connectez-vous à la console NFA.
    b. Cliquez sur Présentation d'entreprise dans le menu principal.
    c. Vérifiez que les vues de rapport affichent les interfaces.

ca technologies **Network Flow Analysis**

Présentation de l'entreprise | Interfaces | Génération de rapports personnalisés | Examen des flux | Analyse | Intersi

Utilisation des interfaces

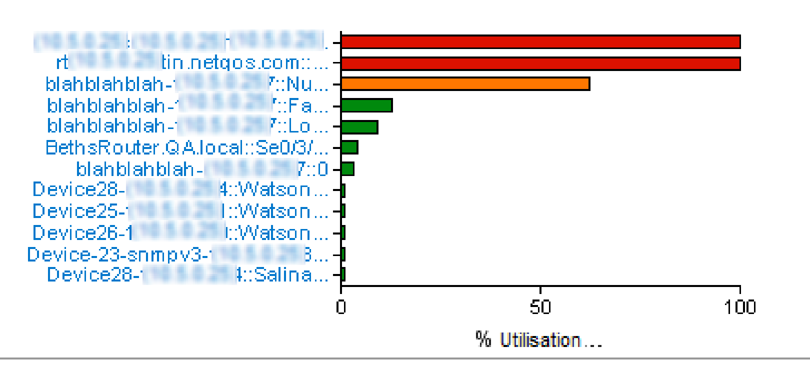
25 janvier 2015 08:45:00 - 26 janvier 2015 08:45:00 GMT

Statut	Interface
■	rtr-5.25-austin.netqos.com::AnotherATM
■	rtr-5.25-austin.netqos.com::AnotherATM

■ Utilisation ≥ 75,00

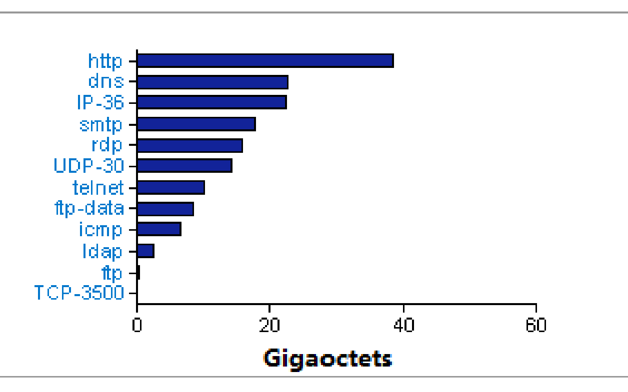
Principales interfaces - En entrée

25 janvier 2015 08:45:00 - 26 janvier 2015 08:45:00 GMT



Principaux protocoles

25 janvier 2015 08:45:00 - 26 janvier 2015 08:45:00 GMT



2. Vérifiez que les interfaces sont visibles dans Interface Index :
   a. Dans le menu de la console NFA, cliquez sur Interfaces.

      L'index d'interface s'ouvre.
   b. Vérifiez qu'il inclut les interfaces que vous pensiez y trouver.

      Vous pouvez développer les détails du routeur pour en afficher les interfaces. Vous pouvez également utiliser la zone de recherche et entrer un nom entier ou partiel ou une description pour rechercher des routeurs ou des interfaces.
3. Si les interfaces ne s'affichent pas dans la console NFA, effectuez la procédure de dépannage préliminaire suivante :
   - Vérifiez que les services CA Network Flow Analysis sont en cours d'exécution sur le serveur de la console NFA.
   - Révisez les journaux. Affichez les journaux dans la console NFA ou ouvrez-les à partir du répertoire <répertoire_installation_>\reporter\Logs.

Modification du domaine des interfaces et des interfaces virtuelles personnalisées

Les interfaces et les interfaces virtuelles personnalisées héritent leur paramètre de domaine de client hébergé initial du routeur parent et du Harvester lors de l'ajout de ce dernier et du lancement de la collecte des données à partir du routeur et des interfaces. Si le Harvester n'est associé à aucun domaine personnalisé, les routeurs et les interfaces sont affectés au domaine par défaut au lancement de la collecte de leurs données.

Vous pouvez modifier les paramètres pour des interfaces et des interfaces virtuelles personnalisées à tout moment. Le paramètre de domaine ne doit pas nécessairement correspondre au routeur ou au Harvester parent. La modification du domaine peut affecter le type d'opérateurs et de rapports ayant accès aux données des interfaces.

Remarque : La fonctionnalité de client hébergé est applicable uniquement aux déploiements qui incluent CA Performance Center. Si votre déploiement utilise CA NetQoS Performance Center, le paramètre de client hébergé est toujours Client hébergé par défaut.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.

      La page Interfaces actives s'ouvre.

2. Identifiez et cochez la case en regard d'une ou de plusieurs interfaces à associer à un domaine de client hébergé.
   - Pour rechercher des routeurs parents, des interfaces ou des interfaces virtuelles personnalisées, entrez tout ou partie de l'adresse IP de routeur, du nom de routeur ou d'interface, ou de la description d'interface dans le champ Rechercher, puis cliquez sur Rechercher. Développez les détails du routeur.
   - Pour accéder à une interface ou à une interface virtuelle personnalisée manuellement, allez à la page qui contient le routeur parent et cliquez sur la flèche à côté du nom du routeur. Les détails du routeur s'étendent et indiquent les interfaces et les interfaces virtuelles personnalisées.
3. Cliquez sur Modifier.

   La boîte de dialogue de modification s'affiche. La liste de sélection Domaine figure dans la boîte de dialogue uniquement s'il existe plusieurs domaines.
4. Dans la liste Domaine, sélectionnez une option de domaine ou de client hébergé.
5. Cliquez sur Enregistrer.

   La boîte de dialogue se ferme. Les modifications sont reflétées dans la page Interfaces actives.

Remarque : Vous pouvez également modifier le paramètre du domaine/client hébergé des Harvesters (page 94) et des routeurs (page 66).

Configuration des interruptions

La configuration des interruptions est terminée une fois que vous avez effectué les tâches suivantes :

- Créez les interruptions dont vous avez besoin. Consultez la rubrique Création d'interruptions du *Manuel de l'administrateur de CA Network Flow Analysis*.
- Activez l'affichage des interruptions sous forme d'événements dans la console CA Performance Center :
  1. Ouvrez la page Paramètres de l'application dans la console NFA.
  2. Définissez la valeur de destination des interruptions de sorte qu'elle corresponde à l'adresse IP d'un des serveurs suivants :
     - (CA PC) Console NFA ou serveur autonome enregistré comme source de données
     - (NPC) Serveur du gestionnaire d'événements
- (Facultatif) Activez l'envoi des notifications d'interruption de l'outil de surveillance à votre récepteur d'interruptions : ouvrez la page Watchdog Settings (Paramètres de l'outil de surveillance) dans la console NFA. Configurez les valeurs des paramètres Trap Destination (destination de l'interruption), Email Address (adresse électronique) et autres paramètres de l'outil de surveillance.

- (Facultatif) Vérifiez que les événements sont affichés dans la console Performance Center, sur la page Evénements (dans CA PC) ou sur la page Event Liste (Liste des événements, dans NPC). Si les événements ne s'affichent pas comme prévu, vérifiez que les conditions suivantes sont remplies :
  - Les fichiers affichent les événements qui ont été générés et qui ont été envoyés au gestionnaire d'événements.
  - Le nom d'hôte du gestionnaire d'événements peut être résolu par le serveur DNS pour CA Network Flow Analysis.
  - La valeur de destination des interruptions dans la page Paramètres de l'application de la console NFA correspond à l'adresse IP d'un des serveurs suivants :
    - (CA PC) Console NFA ou serveur autonome enregistré comme source de données
    - (NPC) Serveur du gestionnaire d'événements
  - (NPC uniquement) : Event Manager (Gestionnaire d'événements) est installé.

Configuration des comptes d'utilisateurs

Un compte d'utilisateur prédéfini (admin) est inclus avec l'installation de CA Network Flow Analysis. Le compte admin possède des droits d'administration complets.

L'administrateur doit créer un compte d'utilisateur pour chaque personne qui utilisera le produit, administrateurs et opérateurs. Les comptes d'utilisateurs personnalisés améliorent la sécurité des produits et bénéficient des droits de rôle strictement définis qui déterminent l'accès des utilisateurs aux différentes fonctionnalités et données des produits.

Il est préférable de déployer les comptes d'utilisateurs personnalisés dans un système planifié de façon appropriée et qui inclut des groupes personnalisés. Les groupes personnalisés sont affectés en tant qu'autorisations pour permettre aux opérateurs du produit d'afficher uniquement les données, menus et tableaux de bord dont ils ont besoin pour effectuer leurs tâches quotidiennes.

Affichage d'une liste des comptes d'utilisateurs

La console CA Performance Center inclut une présentation générale des paramètres des comptes d'utilisateurs. Avant de créer des comptes d'utilisateurs personnalisés, seuls deux comptes d'utilisateurs prédéfinis sont disponibles.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle administratifs requis.

2. Cliquez sur Administration, Paramètres de l'utilisateur : Utilisateurs.

   La liste actuelle des comptes d'utilisateurs est affichée dans la page Gérer les utilisateurs (CA PC) ou User List (Liste des utilisateurs) (NPC).

   La table inclut les informations suivantes concernant chaque compte d'utilisateur :

   Nom

   Nom de connexion pour le compte d'utilisateur.

   Rôle

   Rôle affecté au compte d'utilisateur.

   Droit CAPC/NPC

   Identifie le niveau de l'accès aux sources de données enregistrées, comme CA Network Flow Analysis.

   Autorisation

   Répertorie les groupes d'autorisations affectés à ce compte. Vous pouvez afficher les groupes d'autorisations comme des emplacements imbriqués dans l'arborescence Groupes.

   Par défaut : /Tous les groupes.

   Statut

   Indique si le compte d'utilisateur est activé ou désactivé.

   Remarque : Les valeurs de statut supplémentaires peuvent être répertoriées dans la console pour CA NetQoS Performance Center : intégré (configuré automatiquement) et en ligne (actuellement connecté).

   Pour effectuer une action sur cette page, cliquez sur l'un des boutons du bas.

Ajout de comptes d'utilisateurs

Ajoutez un compte d'utilisateur pour chaque personne qui utilisera les produits. Pour des raisons de sécurité, les opérateurs ne doivent pas partager de comptes d'utilisateurs.

Remarque : Cette rubrique décrit la procédure à suivre pour effectuer cette tâche dans CA Performance Center. Si vous enregistrez CA Network Flow Analysis comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle administratifs requis.
2. Confirmez que les rôles et les groupes requis existent.
3. Sélectionnez Administration, Paramètres de l'utilisateur : Utilisateurs.

   La liste actuelle des comptes d'utilisateurs apparaît.

4. Cliquez sur Créer.

   L'assistant Créer un utilisateur (CA PC) ou la page Add User page (Ajouter un utilisateur) (NPC) s'ouvre.

5. Entrez des informations pour les paramètres suivants :

   Nom

   Nom de connexion pour le compte d'utilisateur. Limité à 50 caractères.

   Description

   (Facultatif) Décrit le compte d'utilisateur pour vous aider à l'identifier.

   Adresse électronique

   (Facultatif) Associe une adresse électronique au compte d'utilisateur.

   Langue préférée (CA PC uniquement)

   Spécifie la langue parlée par l'opérateur associé au compte d'utilisateur.

   Type d'authentification

   Identifie la méthode d'authentification qui s'applique à ce compte d'utilisateur. La méthode doit correspondre à la configuration de l'authentification unique. Sélectionnez l'une des options ci-dessous.

   - Performance Center (CA PC) ou Product (Produit) (NPC) : schéma d'authentification par défaut déployé par CA Performance Center.
   - Externe : un schéma d'authentification tiers, comme LDAP ou SAML.

   Mot de passe

   Définit un mot de passe pour le compte d'utilisateur. Le mot de passe est limité à 32 caractères.

   Fuseau horaire

   Correspond au fuseau horaire dans lequel l'utilisateur affichera des données.

   Par défaut : UTC (Temps universel coordonné).

   Rôle

   Rôle affecté au compte d'utilisateur.

   Statut du compte (CA PC uniquement)

   Détermine si le compte est activé pour l'utilisation (Activé).

   User Options (Options de l'utilisateur) (NPC uniquement)

   Détermine si le compte est activé pour l'utilisation (Activé) et si l'utilisateur est autorisé à partager des vues avec d'autres produits (Permettre aux utilisateurs de générer des URL pour les vues de données).

6. Affectez des autorisations d'accès à l'utilisateur, comme décrit dans la section Affectation de groupes d'autorisations à des comptes d'utilisateurs (page 48).

7. Ajoutez des groupes d'autorisations au compte d'utilisateur, comme décrit dans la section Affectation de droits de produit (page 49).

8. Cliquez sur Enregistrer.

   Le nouvel utilisateur apparaît dans la liste de comptes d'utilisateurs.

Droits de rôle

Les droits affectés à chaque rôle déterminent l'accès de l'utilisateur à des tableaux de bord et à des menus. Par exemple, les droits de rôle contrôlent les types de vues que les utilisateurs peuvent voir et contrôlent si les utilisateurs peuvent exporter des données, personnaliser des paramètres et configurer des planifications pour l'envoi de rapports par courriel.

Les administrateurs peuvent accorder des droits supplémentaires à des utilisateurs en modifiant leur rôle. La boîte de dialogue Modifier le rôle répertorie les droits de rôle actuellement affectés aux rôles. La page Gérer les utilisateurs ou Liste des utilisateurs affiche le rôle affecté à chaque utilisateur.

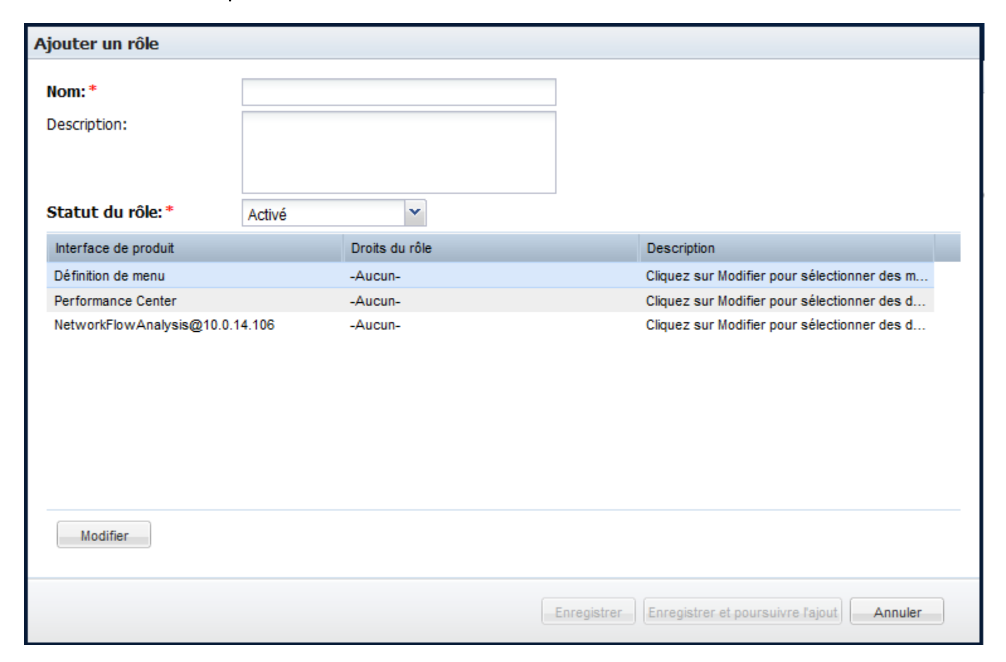
Remarque : Ne supprimez pas les droits de rôle administratifs de votre compte d'administrateur principal. L'accès administratif à la console est requis.

Ajout de droits de rôle pour les utilisateurs

Si les rôles d'utilisateur prédéfinis ne répondent pas à vos besoins, vous pouvez ajouter des rôles d'utilisateur personnalisés. Dans l'idéal, vous créez les rôles dont chaque opérateur de produit unique a besoin pour pouvoir remplir ses responsabilités professionnelles.

Les rôles personnalisés fonctionnent mieux dans un système de groupes personnalisés. Les groupes personnalisés permettent d'accorder précisément un accès aux tableaux de bord et aux fonctionnalités de produit tout en limitant l'accès aux données sensibles. Les mêmes groupes que vous créez pour organiser des données peuvent servir de "groupes d'autorisation" lorsque vous configurez des autorisations de compte d'utilisateur.

Un nouveau rôle n'a des droits que lorsque vous les avez ajoutés. L'illustration suivante représente la boîte de dialogue Ajouter un rôle dans la console CA Performance Center avec un rôle sur le point d'être défini.



Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle administratifs requis.
2. Accédez à la page Gérer les rôles ou Roles List (Liste des rôles).

   La liste actuelle des rôles s'affiche dans cette page.
3. Cliquez sur Créer.

   La boîte de dialogue Ajouter un rôle s'ouvre.

4. Fournissez les informations requises et faites des sélections dans les champs fournis :

   Nom

   (Facultatif) Identifie le rôle. Limité à 45 caractères.

   Description

   (Facultatif) Décrit le rôle. Par exemple, identifie les taxes en rapport avec le travail effectué par l'utilisateur associé.

   Activer le rôle

   Permet d'activer le rôle. Requis pour donner aux utilisateurs disposant de ce rôle l'accès accordé par des droits de rôle.

5. Spécifiez les menus qui seront visibles pour les utilisateurs disposant du nouveau rôle :

   a. Sélectionnez Ensemble de menus (CA PC) ou sélectionnez un menu ou un produit dans la liste au bas de la boîte de dialogue (NPC).

   b. Cliquez sur Modifier.

      La boîte Modifier l'ensemble de menus s'ouvre. Vous pouvez ajouter au rôle des menus répertoriés dans la liste Menus disponibles.

   c. Cliquez sur un élément sur la gauche que vous souhaitez ajouter au rôle, puis cliquez sur la flèche droite.

      Utilisez Maj + clic ou Ctrl + clic pour sélectionner plusieurs éléments.

      Chaque élément sélectionné passe dans la liste Menus sélectionnés.

   d. (Facultatif) Utilisez les flèches vers le haut et vers le bas pour déplacer des éléments dans la liste. L'ordre de menus dans la liste détermine leur ordre sur l'onglet Tableaux de bord.

   e. Cliquez sur OK.

      Vous revenez à la page Ajouter un rôle.

6. Définissez les droits Performance Center pour le rôle :

   a. Sélectionnez Performance Center (CA PC) ou NetQoS Performance Center (NPC).

   b. Cliquez sur Modifier.

      Une boîte de dialogue s'ouvre et vous permet de sélectionner des droits d'accès Performance Center.

   c. Cliquez sur un élément sur la gauche que vous souhaitez ajouter au rôle, puis cliquez sur la flèche droite.

      Le droit d'accès est déplacé dans la liste Droits sélectionnés.

d. (Facultatif) Utilisez les flèches vers le haut et vers le bas pour déplacer des éléments dans la liste. L'ordre des droits de rôle détermine leur priorité en cas de chevauchement de ces droits.

e. Cliquez sur OK.

   Vous revenez à la page Ajouter un rôle.

7. Définissez les droits CA Network Flow Analysis pour le rôle :

   a. Sélectionnez le nom de l'instance CA Network Flow Analysis enregistrée.

   b. Cliquez sur Modifier.

      Une boîte de dialogue s'ouvre et vous permet de sélectionner des droits d'accès pour CA Network Flow Analysis de la même façon que vous en avez sélectionné pour Performance Center.

   c. Une fois que les droits d'accès sont configurés, cliquez sur OK.

      Le nouveau rôle est créé et apparaît dans la Liste des rôles.

8. Répétez l'étape précédente pour définir les droits pour toute source de données supplémentaire que vous voulez inclure.

9. Cliquez sur Enregistrer dans la page Ajouter un rôle.

   Vous revenez à la page Gérer les rôles (CA PC) ou Roles List (Liste des rôles) (NPC).

Remarque : Après avoir créé un rôle, vous devez l'affecter à un compte d'utilisateur au cours d'une autre étape. Les rôles deviennent actifs après leur affectation à des comptes d'utilisateurs. Seuls les utilisateurs disposant du rôle Administrer les utilisateurs peuvent affecter des rôles à des comptes d'utilisateurs.

Affectation de groupes d'autorisations à des comptes d'utilisateurs

Les différents opérateurs requièrent des autorisations d'accès aux données afin de surveiller ces dernières dans les produits. Les autorisations d'accès sont basées sur des groupes. Vous pouvez affecter des autorisations d'accès en fonction de votre plan pour les groupes personnalisés. Votre objectif, en tant qu'administrateur, est de vous assurer que tous les opérateurs consultent uniquement les données dont ils ont besoin.

Par exemple, supposez que vous créez des groupes personnalisés et les affectez comme des autorisations au personnel informatique. Lorsque les membres du personnel se connectent à CA Performance Center, ils peuvent afficher des données des systèmes qui leur sont affectés.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur possédant des droits d'administration.
2. Cliquez sur Administration, Paramètres de l'utilisateur : Utilisateurs.

   La page Gérer les utilisateurs (CA PC) ou User List (Liste des utilisateurs) (NPC) s'ouvre.
3. Sélectionnez un compte d'utilisateur à modifier et cliquez sur Modifier.

   L'assistant ou la boîte de dialogue de modification d'un utilisateur s'ouvre.
4. Affichez les groupes d'autorisations :
   - (CA PC) Cliquez sur le bouton Droits d'accès.
   - (NPC) Repérez le volet Permission Groups (Groupes d'autorisations) au milieu de la page.

   Les paramètres de groupe s'affichent.
5. Ajout de groupes d'autorisations au compte d'utilisateur
   - Développez les groupes dans l'arborescence Groupes disponibles sur la gauche pour que les sous-groupes s'affichent.
   - Sélectionnez un groupe ou un sous-groupe.
   - Cliquez sur la flèche vers la droite ou sur le bouton Add (Ajouter) pour ajouter le groupe.
   - Répétez cette opération si nécessaire.

   Les groupes d'autorisations sélectionnés s'affichent dans le volet Groupes sélectionnés.

6. Sélectionnez le groupe par défaut pour l'utilisateur, autrement dit les données qui s'affichent par défaut dans les tableaux de bord pour l'utilisateur :
   - (CA PC) Cliquez avec le bouton droit de la souris sur le groupe cible et sélectionnez Définir en tant que valeur par défaut.
   - (NPC) Sélectionnez le groupe cible et cliquez sur Make Default (Définir en tant que valeur par défaut).
7. Cliquez sur Enregistrer.

   Les modifications sont enregistrées dans le compte d'utilisateur, et vous revenez à la page Gérer les utilisateurs.

   Lorsque l'utilisateur se connecte, les données provenant du groupe par défaut s'affichent dans des tableaux de bord par défaut.

Affectation de droits de produit

Chaque source de données dispose de ses propres droits de produit, notamment des droits uniques pour l'interface correspondante. Les administrateurs confèrent des droits de produit aux utilisateurs pour chaque source de données. Par exemple, le droit d'accès au produit détermine si un utilisateur est autorisé à se connecter à CA Network Flow Analysis ou à effectuer une navigation descendante à partir d'une vue CA Performance Center et vers les détails dans la console NFA. Les droits sont spécifiques à l'instance de source de données.

Le compte d'administrateur par défaut (admin), est verrouillé pour empêcher toute modification des droits du produit. Ce compte doit disposer de droits d'administrateur pour toutes les sources de données enregistrées. Si vous sélectionnez un groupe de comptes qui inclut le compte d'administrateur, vous ne pouvez pour modifier les droits du produit pour aucun des comptes sélectionnés.

Droits du produit CA Network Flow Analysis

Pour pouvoir se connecter à la console NFA, les utilisateurs doivent disposer de droits d'accès au produit sur la source de données CA Network Flow Analysis. Les droits d'accès au produit permettent également d'autoriser un utilisateur à accéder à la page Administration et à effectuer des fonctions spécifiques :

Administrateur

Permet d'accéder à la page Administration de la console NFA et à toutes les fonctions. Les fonctions incluent la création et la gestion des comptes d'utilisateurs, des rôles, des groupes, des profils SNMP et de la planification pour les rapports.

Utilisateur avancé

Fournit un accès de niveau utilisateur et les droits accordés par le paramètre Rôle. Pour CA Network Flow Analysis, le droit Utilisateur avancé est équivalent au droit Administrateur.

User (Utilisateur)

Permet d'accéder aux rapports sur les principales interfaces et l'utilisation des interfaces dans la page Enterprise Overview (Présentation de l'entreprise).

Un utilisateur avec les paramètres Groupe d'autorisations appropriés peut accéder aux rapports suivants :

- Rapports Principaux hôtes et Principaux protocoles de la page Présentation de l'entreprise, à condition que l'utilisateur ait également accès à tous les groupes.
- Rapports de la page Interfaces pour les interfaces accessibles à l'utilisateur.
- Rapports existants dans les pages Custom Reporting, Flow Forensics et Analysis
- Menus qu'un administrateur a affectés au rôle d'utilisateur

Les paramètres Groupe d'autorisations et Rôle déterminent si l'utilisateur peut exécuter également les rapports existants, créer des rapports et gérer des rapports. Pour créer des rapports, un utilisateur doit avoir accès à tous les groupes.

Aucun

N'a pas accès à une source de données. Les utilisateurs qui possèdent un droit d'accès au produit ne peuvent pas se connecter à la console NFA ni passer d'une vue CA Performance Center à la console NFA. Par défaut, tous les utilisateurs possèdent ce paramètre de droit du produit pour toutes les sources de données.

Remarque : Le même compte d'utilisateur peut avoir des droits différents pour des sources de données différentes.

Configuration des groupes

Nous vous recommandons de créer des groupes personnalisés pour faciliter la gestion des éléments dans la console CA Performance Center. Des groupes personnalisés sont requis pour permettre aux opérateurs d'afficher des données concernant les performances des routeurs qu'ils gèrent.

S'ils sont correctement configurés, les groupes peuvent empêcher les opérateurs d'afficher certaines données pour des raisons de sécurité. L'administrateur peut autoriser certains utilisateurs à accéder aux données qui appartiennent à leur zone de responsabilité, un emplacement physique ou un sous-réseau par exemple.

Création de groupes personnalisés

Avant de commencer à créer des groupes, planifiez une stratégie et une structure. Considérez les types d'autorisations d'accès dont les opérateurs ont besoin pour effectuer leurs tâches de surveillance. Si nécessaire, vous pouvez discuter vos objectifs en termes d'organisation et de surveillance avec un représentant technique CA.

Créez des groupes sous le noeud Tous les groupes dans l'arborescence de groupes, ou dans un groupe de sites ou un groupe personnalisé existant. Vous ne pouvez pas ajouter de groupes à des groupes système qui apparaissent "verrouillés" dans l'arborescence Groupes.

Vous pouvez ajouter un maximum de 2000 groupes enfants à un groupe parent.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle administratifs requis.
2. Accédez à la page Gérer les groupes.

   La page affiche des groupes actuels dans une arborescence.
3. Développez des noeuds dans l'arborescence de groupes pour trouver un emplacement pour le nouveau groupe.
4. Cliquez avec le bouton droit de la souris sur le noeud, puis sélectionnez Ajouter un groupe (CA PC) ou Add New Group (Ajouter un nouveau groupe) (NPC).

   La fenêtre Ajouter un groupe s'ouvre : l'onglet Créer y est sélectionné par défaut.
5. Fournissez des valeurs pour les paramètres suivants :

   Nom du groupe

   Spécifie un nom pour le groupe. N'utilisez pas les caractères spéciaux suivants dans des noms de groupe : /&\,%.

   Description

   (Facultatif) Vous aide à identifier le groupe.
6. Confirmez la valeur du paramètre suivant :

   Inclure les enfants des éléments gérés

   Ajoute automatiquement les enfants des éléments gérés lorsque les éléments sont ajoutés à ce groupe. Si cette option est désactivée et que vous ajoutiez un routeur, les interfaces de routeur ne seront pas incluses. En conséquence, les données de ces interfaces ne sont pas affichées dans les vues détaillées.

   Valeur par défaut : Option sélectionnée (CA PC) ou non sélectionnée (NPC).

   Remarque : Effacez cette option pour un groupe personnalisé qui contient des routeurs ou le groupe ne sera pas utilisable dans la console NFA.

7. Sélectionnez Personnalisé ou Par site dans la liste de Type de groupe.

   Si vous avez sélectionné Site comme type, spécifiez des valeurs pour les paramètres supplémentaires qui s'affichent, y compris l'emplacement.

8. Cliquez sur Enregistrer.

   Le nouveau groupe apparaît dans l'arborescence Groupes.

   Il ne contient aucun élément. Deux options sont disponibles pour ajouter des éléments à un groupe personnalisé :

   - Remplissez manuellement le groupe en ajoutant des éléments dans l'interface Gérer les groupes.
   - Créez des règles pour gérer l'appartenance aux groupes.

Résultats de l'annulation de l'enregistrement

Il se peut exceptionnellement que vous souhaitiez annuler l'enregistrement de CA Network Flow Analysis, par exemple, avant d'enregistrer une instance CA Network Flow Analysis avec une instance CA Performance Center différente, vous devez annuler l'enregistrement de cette instance CA Network Flow Analysis. Annulez l'enregistrement uniquement si c'est vraiment nécessaire.

Si vous annulez l'enregistrement de CA Network Flow Analysis, les règles suivantes s'appliquent :

- Utilisateurs : les utilisateurs qui ne sont pas associés à CA Network Flow Analysis sont supprimés. Les ID d'utilisateurs existants sont conservés. Vous ne pouvez pas ajouter de nouveaux utilisateurs ni modifier les paramètres des comptes d'utilisateurs si l'enregistrement est annulé.
- Rôles : les rôles ne sont pas supprimés. Les utilisateurs conservent leurs rôles précédents. Les ID de rôles existants sont conservés. Vous ne pouvez pas modifier les rôles ou les autorisations pour les utilisateurs existants si l'enregistrement est annulé.

- Groupes :
  - les groupes qui n'existent pas dans CA Network Flow Analysis sont supprimés. Vous ne pouvez pas ajouter ni modifier de groupes si l'enregistrement est annulé.
  - Les groupes imbriqués qui sont associés à une interface sont affichés en tant que groupes d'interfaces dans la console NFA.
  - Les groupes qui ne sont associés à aucune interface apparaissent en tant qu'autorisations.
- Authentification unique et LDAP : l'authentification unique et les valeurs LDAP sont conservées.

Remarque : Pour obtenir une description plus détaillée des résultats d'annulation de l'enregistrement lors d'une mise à niveau de CA Network Flow Analysis, consultez le *Manuel de mise à niveau de CA Network Flow Analysis*.

Tâches de post-installation

Vous pouvez effectuer plusieurs tâches d'administration supplémentaires, selon votre environnement et le nombre d'utilisateurs. Nous vous recommandons de réaliser certaines tâches dès l'exécution de CA Network Flow Analysis. Considérez les tâches suivantes :

- **Vérification de la configuration des paramètres requis**

  Vérifiez que toutes les tâches d'installation sont terminées. Certains paramètres sont requis pour activer certaines fonctionnalités, comme l'envoi de rapports par courriel et le déclenchement des interruptions SNMP.

- **Ajustement des paramètres pour améliorer les performances**

  Certains paramètres des rapports peuvent affecter les performances, comme la fréquence de la résolution du nom d'hôte DNS.

- **Vérification des vitesses d'interface**

  Si l'utilisation des interfaces dans la console NFA atteint 100 % ou les dépasse (par exemple, comme dans la page Présentation d'entreprise), vous pouvez ajuster les vitesses d'interface. Pour obtenir des informations supplémentaires sur la modification des paramètres d'interface, reportez-vous à la rubrique Expiration des adresses caduques (page 172).

- **Contrôle de l'affichage de routeur**

  Vous pouvez exclure des domaines de l'affichage pour contrôler les routeurs affichés dans la console NFA.

  Remarque : Cette action est applicable uniquement dans un déploiement qui inclut plusieurs domaines.

- **Désactivation de la surveillance du trafic généré par les routeurs**

  Si vous ne souhaitez pas que les rapports incluent le trafic d'émission pour chaque routeur, définissez le paramètre d'application Pompage de l'émission ou de la multidiffusion sur False.

- **Surveillance de composants de produit**

  Les services de surveillance vous permettent de surveiller les composants. Vérifiez que les paramètres appropriés sont configurés pour notifier des problèmes de composant dès leur apparition. Spécifiez notamment les seuils ou encore l'adresse électronique à laquelle les messages doivent être envoyés. Pour obtenir des informations supplémentaires, reportez-vous à la rubrique Surveillance des composants de CA Network Flow Analysis (page 162).

- **Ajustement des paramètres de sécurité**

  Pour exporter des rapports dans des fichiers *CSV*, les paramètres de sécurité de votre environnement peuvent rendre nécessaire l'ajout de l'adresse IP de la console NFA à votre liste de sites de confiance.

Remarque : Pour obtenir des informations sur l'installation et la mise à niveau, consultez les manuels suivants :

- *Manuel d'installation de CA Network Flow Analysis*
- *Manuel de mise à niveau de CA Network Flow Analysis*

Chapitre 3: Options de la page Administration

La page Administration de CA Network Flow Analysis vous permet de consulter, d'administrer et de personnaliser l'affichage des données de réseau. Le statut du système est indiqué dans cette page à l'ouverture de celle-ci. Il est indiqué au moyen des icônes suivantes :

- Coche *verte* : le composant s'exécute sans erreurs.
- Point d'exclamation *rouge* : le composant s'exécute, mais des erreurs sont détectées.

Cliquez sur le point d'exclamation rouge pour afficher le rapport d'erreur correspondant. Le rapport d'erreur inclut l'adresse IP, le type de composant et d'autres d'informations sur l'erreur. Aucun message d'erreur n'est affiché pour la coche verte.

Remarques :

- Pour effectuer des tâches d'administration, connectez-vous en tant qu'utilisateur possédant des droits d'administrateur.
- Certaines options vous mènent à une page de la console correspondant à la version de Performance Center que vous utilisez avec CA Network Flow Analysis. Si le produit est enregistré en tant que source de données pour CA Performance Center ou pour CA NetQoS Performance Center, les options suivantes sont activées :
  - Groupes CA Performance Center ou groupes NPC
  - Utilisateurs
  - Rôles
  - Profils SNMP

Un menu d'options d'administration se trouve sur le côté gauche de la page. La liste suivante décrit les pages et les fonctions qui correspondent aux options.

Menu Interfaces

Physique et virtuelle

Visualisez le statut des interfaces dans la page Interfaces actives. Vous pouvez également modifier, supprimer ou fusionner des interfaces ou créer et modifier des interfaces virtuelles personnalisées.

Agrégations

L'agrégation d'interfaces s'effectue dans la page Agrégations d'interfaces. Les agrégations d'interface permettent d'afficher et de générer des rapports sur les interfaces en tant que groupe unifié.

Menu Alertes

Alertes

Révisez, ajoutez, modifiez et supprimez des interruptions dans la page Configuration des interruptions.

Définir une application : sous-menu Groupes

Définitions d'application

Créez et modifiez des règles pour le mappage d'applications, des priorités de port ou des places réservées dans la page Définitions d'applications.

Noms de protocole

Utilisez la page Configuration du protocole pour modifier les noms et descriptions des protocoles. Dans un déploiement qui inclut plusieurs domaines, les noms de protocole sont propres au domaine.

Noms de types de service

La modification d'une étiquette de type de service (description) dans le contexte d'un domaine spécifique s'effectue dans la page Configuration du type de service. Vous pouvez en outre ajouter, supprimer ou modifier des groupes de valeurs de type de service. Dans un déploiement qui inclut plusieurs domaines, les noms de types de service sont propres au domaine.

Noms AS

La page Noms des systèmes autonomes permet de rechercher et de modifier des noms de systèmes autonomes dans le contexte d'un domaine spécifique. Dans un déploiement qui inclut plusieurs domaines, les noms de systèmes autonomes sont propres au domaine.

Groupes de types de service

Vérifiez, ajoutez, modifiez ou supprimez des groupes de types de service dans la page Configuration du groupe de types de service.

Groupes de protocoles

Vérifiez, ajoutez, modifiez ou supprimez des groupes de protocoles dans la page Configuration du groupe de protocoles.

Administration : sous-menu Génération de rapports

Groupes CA Performance Center ou groupes NPC

Dans la console Performance Center, ouvrez la page Gérer des groupes. Révisez les groupes système et ajoutez, supprimez, ou modifiez des groupes personnalisés et des groupes par site. Cette option est activée si CA Network Flow Analysis est enregistré en tant que source de données au niveau de Performance Center.

Périodes de génération de rapports

Utilisez la page Configuration des périodes de génération de rapports pour ajouter, modifier et supprimer des périodes de génération de rapports. Les opérateurs peuvent utiliser les périodes de génération de rapports pour limiter les périodes des données dans les rapports d'interface.

Filtres de temps

Affichez, ajoutez, modifiez et supprimez des filtres de temps dans la page Configuration du filtre de temps.

Courriels planifiés

Utilisez la page Courriels planifiés pour réviser les rapports planifiés pour la remise de courriels. Vous pouvez modifier l'adresse de destination, l'objet, le texte du message associé et les options de planification.

Adresses

Utilisez la page Configuration de l'adresse ou du nom d'hôte pour spécifier un masque et définir les options de résolution des adresses IP en noms DNS. Vous pouvez répertorier, modifier, supprimer et faire expirer des adresses IP. L'expiration des adresses IP entraîne la planification de leur actualisation. Dans un déploiement qui inclut plusieurs domaines, la configuration de l'adresse est propre au domaine.

Administration : sous-menu Authentification

Utilisateurs

Cette page permet de gérer les comptes d'utilisateurs dans la console Performance Center. Révisez les comptes d'utilisateurs et leurs paramètres. Ajoutez, supprimez et modifiez des comptes d'utilisateurs. Cette option est activée si le produit est enregistré en tant que source de données au niveau de Performance Center.

Rôles

Cette page permet de gérer les rôles dans la console Performance Center. Révisez les noms de rôle existants ainsi que les fonctionnalités et les menus disponibles pour chaque rôle. Ajoutez, supprimez et modifiez des rôles. Cette option est activée si le produit est enregistré en tant que source de données au niveau de Performance Center.

Administration : sous-menu Système

Activation des interfaces

Affichez la liste et le statut des routeurs sur la page Interfaces disponibles. Activez, désactivez ou supprimez des interfaces sur cette page.

Harvester

Utilisez la page Harvester pour afficher, ajouter, modifier et supprimer les Harvesters qui génèrent des données de rapport.

 **DSA**

Déploiements d'architecture à trois niveaux uniquement : utilisez la page DSA pour ajouter un DSA à votre configuration ou modifier l'adresse IP d'un DSA. Dans un déploiement d'architecture à trois niveaux, un ou plusieurs DSA stockent les données de résolution en 15 minutes (historique) pour les rapports.

Paramètres d'application

Modifiez une série de paramètres d'application à partir de la page Paramètres de l'application.

Profils SNMP

Cette page permet de gérer les profils SNMP dans la console Performance Center. Affichez, ajoutez, modifiez, supprimez et réorganiser les profils SNMP que les Harvesters utilisent pour l'interrogation. Dans un environnement d'hébergement multiclient, un Harvester utilise les profils SNMP qui sont affectés à son client hébergé. Cette option est activée si le produit est enregistré en tant que source de données au niveau de Performance Center.

Modèles

Utilisez la page Modèles d'interface pour afficher, ajouter, modifier et supprimer des modèles qui déterminent l'affichage des noms et des descriptions des interfaces.

Administration : menu Intégrité

Statut du système

Affichez le statut global des composants CA Network Flow Analysis dans la page Statut du système. Cliquez sur une icône d'avertissement pour afficher une liste des rapports de problème disponibles pour le composant.

Le statut des DSA est utile uniquement pour les déploiements d'architecture à trois niveau. Les DSA ne sont pas incluses dans les déploiements à deux niveaux. Dans un déploiement à deux niveaux, le statut de DSA indique toujours une icône de statut du système verte.

Paramètres de l'outil de surveillance

Affichez et modifiez les paramètres de configuration de l'outil de surveillance à partir de la page Paramètres de l'outil de surveillance.

Menu Anomaly Detector

Anomaly Detector

La fenêtre Anomaly Detector inclut des fonctions permettant d'effectuer des tâches d'administration pour CA Anomaly Detector. Ces fonctions ont été ajoutées à la console NFA pour simplifier le déploiement du produit avec CA Performance Center.

Remarques :

- Si votre déploiement inclut CA NetQoS Performance Center, les mêmes fonctions sont disponibles dans cette Console. Les fonctions présentes dans les deux produits enregistrent vos paramètres dans la même base de données.

  Pour un déploiement de CA NetQoS Performance Center, il est conseillé d'utiliser les fonctions dans la console CA NetQoS Performance Center. Travailler de manière centralisée permet de réduire la possibilité pour plusieurs utilisateurs d'écrire simultanément dans la base de données, Dans le cas contraire, des résultats inattendus peuvent se produire.

La fenêtre Anomaly Detector comporte les onglets suivants :

- Afficher les produits surveillés : permet d'ajouter des produits à faire surveiller par CA Anomaly Detector et de consulter la liste des produits surveillés.

  Les autres fonctions de la page deviennent disponibles une fois que vous ajoutez une instance de CA Network Flow Analysis à surveiller.

- Afficher les sources de collection : permet d'afficher, d'activer et de désactiver les sources de collection surveillées par CA Anomaly Detector.
- Afficher les détecteurs : permet d'afficher et de modifier les paramètres de configuration par défaut des détecteurs.
- Afficher les cibles d'alerte : permet de configurer des cibles d'alerte pour snmp_traps et syslogging.

Pour plus d'informations sur ces fonctions, reportez-vous au *Guide d'CA Anomaly Detector*.

Menu A propos de

A propos de

Pour connaître le numéro de version et la date d'installation du produit, accédez à la page Informations sur la version. Cette page contient également des liens vers l'historique des versions de produit, vers le Manuel de l'administrateur et vers le Manuel de l'opérateur.

Chapitre 4: Utilisation des interfaces et des routeurs

Différentes pages permettent d'effectuer des opérations au niveau des interfaces et des routeurs :

Page Interfaces actives

La page Interfaces actives affiche les interfaces, les routeurs, les interfaces virtuelles personnalisées et les agrégations d'interfaces. Elle inclut uniquement les routeurs et les interfaces qui ont été utilisés pour la collecte des données. Vous pouvez créer et supprimer des interfaces virtuelles personnalisées, fusionner des interfaces et modifier des propriétés. Vous pouvez également supprimer des routeurs et des interfaces sans les supprimer entièrement du système, par exemple pour résoudre des problèmes de capacité.

Dans la page Administration, sélectionnez Interfaces : Physiques et virtuelles, puis, dans la page Interfaces actives, effectuez les principales opérations suivantes :

- Affichage des détails (page 62)
- Modification des détails (page 66)
- Suppression des interfaces (page 70) ou des routeurs (page 68) dans la page
- Création d'interfaces virtuelles personnalisées (page 73)
- Fusion d'interfaces (page 76)

Page Interfaces disponibles

La page Interfaces disponibles affiche les informations concernant l'ensemble des interfaces et des routeurs, y compris celles et ceux qui n'ont à aucun moment été utilisés pour la collecte des données. Vous pouvez activer ou désactiver des interfaces, supprimer des routeurs et leurs interfaces du système et réaliser des opérations de dépannage au niveau de l'interrogation.

Dans la page Administration, sélectionnez Système : Activation d'interfaces, puis, dans la page Interfaces disponibles, effectuez les opérations suivantes :

- Vérification de l'exécution de l'interrogation et affichage des détails concernant les routeurs (page 79) et les interfaces (page 81)
- Activation ou désactivation des interfaces (page 82)
- Suppression des routeurs en fin de vie dans le système (page 83)

Page Modèles d'interface

Vous pouvez créer un modèle d'interface personnalisé pour modifier l'apparence des noms et des descriptions des interfaces dans plusieurs rapports.

Dans la page Administration, sélectionnez Système : Modèles, puis, dans la page Modèles d'interface, effectuez les opérations suivantes :

- Création et application d'un modèle (page 84)
- Modification d'un modèle (page 86)

Page Paramètres de l'application

La page Paramètres de l'application inclut un paramètre permettant de déterminer si les noms d'unité doivent être inclus dans les noms d'interface.

Sélectionnez Paramètres de l'application, puis, dans la page homonyme, effectuez l'opération suivante :

- Ajout ou suppression du nom d'unité dans les noms d'interface (page 87)

Page Interfaces actives

La page Interfaces actives permet d'afficher les routeurs, les interfaces, les interfaces virtuelles personnalisées et les agrégations d'interfaces. Elle inclut uniquement les routeurs et les interfaces qui ont été utilisés pour la collecte des données. Les opérations suivantes sont possibles dans la page Interfaces actives :

- Révision des routeurs, des interfaces et d'autres éléments avec masquage des routeurs et des interfaces qui n'ont jamais été utilisés pour la collecte des données
- Création et suppression des interfaces virtuelles personnalisées
- Fusion d'interfaces
- Suppression d'agrégations d'interfaces
- Suppression de routeurs et d'interfaces pour récupérer de la capacité, tout en les conservant dans la page Interfaces disponibles
- Modification des propriétés, notamment celles ci-dessous :
  - Nom du routeur, domaine, profil ou version SNMP assignés, port et modèle de nommage de l'interface
  - Nom de l'interface, description, vitesse, type et domaine
  - Nom de l'interface virtuelle personnalisée, description, vitesse, type, domaine et sous-réseaux

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.

      La page Interfaces actives s'ouvre.

La page Interfaces actives inclut les options suivantes :

Rechercher

Utilisez une chaîne de texte pour rechercher des routeurs, des interfaces ou d'autres éléments dont l'adresse ou le nom correspond à la chaîne (page 65).

Modifier

Modifiez les propriétés des éléments sélectionnés (page 66).

Supprimer

Supprimez des routeurs (page 68) et des interfaces (page 70) de la page, par exemple pour résoudre des problèmes de capacité.

Fusionner

Combinez les données de deux interfaces physiques ou interfaces virtuelles personnalisées sélectionnées (page 76).

Ajouter une interface virtuelle personnalisée

Créez une interface virtuelle personnalisée à partir de l'interface physique sélectionnée.

Interfaces actives : informations sur les routeurs

Les routeurs sont répertoriés dans les tables de la page Interfaces actives. Les tables de routeur contiennent les colonnes suivantes.

Statut du flux 

Statut du routeur lors de la dernière tentative d'interrogation :

- Rouge : les interfaces activées n'ont pas reçu de flux pendant une durée supérieure à la **limite d'absence de données d'interface**.
- Jaune : les interfaces activées n'ont pas reçu de flux au cours de la durée comprise entre les 30 dernières minutes et la **limite d'absence de données d'interface**.
- Vert : toutes les interfaces activées ont reçu un flux au cours des 30 dernières minutes.

Adresse du routeur

Adresse IP du routeur

Nom du routeur

Nom de routeur assigné par l'utilisateur, par exemple *routeur labo1*

Modèle

Modèle de nommage d'interface assigné

Interfaces

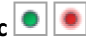
Nombre total d'interfaces, d'agrégations d'interfaces et d'interfaces virtuelles personnalisées du routeur. Ce nombre inclut uniquement les interfaces qui ont été utilisées pour la collecte des données. Pour connaître la liste de toutes les interfaces, allez à la page Interfaces disponibles (page 78).

Harvester

Adresse IP du Harvester chargé de la collecte des données provenant du routeur

Interfaces actives : informations sur les interfaces

Les interfaces et les interfaces virtuelles personnalisées sont répertoriées dans la page Interfaces actives, dans des tables imbriquées sous leurs routeurs parents. Pour afficher les interfaces d'un routeur, cliquez sur la flèche à côté du nom de routeur. Les tables d'interface contiennent les colonnes suivantes.

Statut du trafic 

Statut de l'interface lors de la dernière interrogation :

- Rouge : interface inactive.
- Vert : interface active.

Classe

Icône indiquant le type de l'interface : interface physique, interface virtuelle personnalisée ou agrégation d'interfaces. Pour connaître le type d'une interface, placez le curseur de votre souris sur l'icône.

Nom de l'interface

Nom assigné par l'utilisateur à l'interface, à l'interface virtuelle personnalisée, ou à l'agrégation d'interfaces

Description

Informations facultatives incluses à des fins d'identification

Index des interfaces

Valeur d'index assignée par l'unité qui envoie des flux à l'interface

Type

Type de connexion (WAN ou LAN)

Vitesse en entrée

Vitesse à l'entrée de l'interface, si elle est connue

Vitesse en sortie

Vitesse à la sortie de l'interface, si elle est connue

Domain (Domaine)

Domaine de l'interface. Si l'environnement comprend un seul domaine, la colonne Domaine n'est pas affichée.

Remarques

Ajoutez un lien pour ajouter, modifier ou afficher des remarques relatives à une interface. Si la remarque est vide, l'icône Notes est grisée. Par exemple, vous pouvez ajouter des informations concernant le fuseau horaire, l'unité commerciale, l'emplacement géographique, la bande passante alternative, l'ID de circuit ou l'historique. Les icônes Notes cessent d'être grisées lorsque vous entrez des informations et que vous actualisez la page.

Pour afficher l'icône Notes, accédez à la page Paramètres de l'application et définissez la valeur Afficher le champ Commentaires sur True.

Recherche d'un routeur ou d'une interface

Utilisez la fonction de recherche de la page Interfaces actives pour localiser des routeurs, des interfaces ou des interfaces virtuelles personnalisées. Pour rechercher des agrégations, utilisez la fonction de recherche de la page Interfaces d'agrégation.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.

   La page Interfaces actives s'ouvre.
2. Introduisez une chaîne de texte dans le champ Rechercher. Recherchez des chaînes de texte entières ou partielles qui correspondent aux adresses, aux noms ou aux descriptions de routeurs, d'interfaces ou d'interfaces virtuelles personnalisées.

   Remarque : N'utilisez pas de caractères génériques.

3. Cliquez sur Rechercher.

   La liste est filtrée afin d'afficher uniquement les entrées correspondantes. Si vous recherchez des interfaces ou des interfaces virtuelles personnalisées, la recherche renvoie une liste de routeurs qui contiennent les éléments correspondants. Lorsque vous développez les détails d'un routeur, tous les éléments s'affichent dans les sous-listes.

Pour effacer la recherche, cliquez sur Effacer le filtre.

Modification des détails d'un routeur et d'une interface

Vous pouvez modifier les propriétés d'un routeur ou d'une interface, notamment afin de corriger des informations ou de fournir des informations manquantes.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.

      La page Interfaces actives s'ouvre.

2. Localisez les routeurs, les interfaces ou les autres éléments de votre choix. Pour afficher le contenu d'un routeur, cliquez sur la flèche à côté du nom du routeur.
3. Cochez la case à cocher située près des éléments à modifier. Vous pouvez modifier plusieurs interfaces et interfaces virtuelles personnalisées à la fois, ou modifier plusieurs routeurs à la fois. Toutefois, vous ne pouvez pas modifier simultanément plusieurs routeurs, interfaces ou interfaces virtuelles personnalisées.
4. Cliquez sur Modifier.

   La boîte de dialogue s'ouvre pour permettre la modification des éléments sélectionnés.

5. Modifiez les propriétés de votre choix, par exemple celles ci-dessous :
   - Nom du routeur, domaine du client hébergé (le cas échéant), profil SNMP/version, port et modèle

     (Déploiement de CA PC) Les options de modification du profil et du port SNMP sont activées dès qu'une combinaison client hébergé/domaine est sélectionnée.

- Nom de l'interface, description, vitesse, type de connexion et domaine (le cas échéant)

  Remarques :

  - Vous pouvez également modifier les propriétés des interfaces virtuelles personnalisées et des agrégations.
  - Si vous sélectionnez plusieurs éléments à modifier, les options de modification sont limitées aux propriétés partagées de ces éléments.
  - Le paramètre client hébergé/domaine des interfaces ne doit pas obligatoirement correspondre au paramètre du routeur parent. La modification du domaine peut affecter le type d'opérateurs et de rapports ayant accès aux données associées.
  - La modification du client hébergé d'un routeur dans CA Performance Center peut affecter les profils SNMP disponibles pour l'interrogation des interfaces du routeur. Cette limitation n'est pas applicable à CA NetQoS Performance Center, qui utilise la même liste de profils SNMP pour tous les routeurs.

6. Cliquez sur Enregistrer.

   La boîte de dialogue Modifier le routeur ou Modifier l'interface se ferme. Les modifications sont reflétées dans la page Interfaces actives.

Remarques :

- Si vous supprimez une interface sans la désactiver, elle sera automatiquement ajoutée de nouveau dès qu'elle commencera à envoyer des flux.
- Pour plus d'informations sur la suppression des interfaces et des routeurs, reportez-vous aux rubriques suivantes :
  - Suppression d'une interface (page 70)
  - Suppression d'un routeur dans la page Interfaces actives (page 68)
  - Suppression d'un routeur dans la page Interfaces disponibles (page 83)

Suppression d'un routeur de la page Interfaces actives

Vous pouvez supprimer un routeur sur la page Interfaces actives, tout en le conservant sur la page Interfaces disponibles. Appliquée à un routeur, cette méthode peut permettre de résoudre les problèmes de capacité. Vous pouvez, par la suite, restaurer le routeur (mais pas ses données historiques) en activant ses interfaces sur la page Interfaces disponibles.

La suppression d'un routeur supprime ses interfaces, ses interfaces virtuelles personnalisées, ses données (historiques) de résolution en 15 minutes et ses interruptions. Elle assigne également l'ensemble des agrégations, des vues et des rapports associés.

Remarque : Si vous supprimez le routeur de la page Interfaces disponibles, le système ne possède aucun autre enregistrement du routeur.

Procédez comme suit :

1. Vérifiez que le routeur n'envoie plus de flux au produit.
2. Désactivez les interfaces de routeur, le cas échéant :
   a. Ouvrez la page Interfaces disponibles :
      - Dans le menu de console NFA, sélectionnez Administration.

        La page Administration s'ouvre.
      - Dans le menu Administration, sélectionnez Système : Activer.

        La page Interfaces disponibles s'ouvre.

   b. Localisez le routeur à l'aide de la fonction de recherche ou en navigant dans le contenu de la table.

   c. Cochez la case à côté du routeur.

      Vous pouvez sélectionner et désactiver plusieurs routeurs simultanément, mais ils doivent pour cela se trouver sur la même page.

   d. Cliquez sur Désactiver.

      Un message de confirmation s'affiche.

   e. Cliquez sur Yes (Oui).

      Le statut Activé des interfaces devient Non. Les nouvelles données envoyées par les interfaces ne sont plus collectées ni affichées dans les rapports. Les données déjà collectées peuvent toujours être utilisées pour la génération d'un rapport.

   f. (Facultatif) Mettez à jour la valeur Activé du routeur en actualisant la page, par exemple en appuyant sur la touche F5.

3. Ouvrez la page Interfaces actives :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.

      La page Interfaces actives s'ouvre.
4. Localisez le routeur et activez sa case à cocher.
5. Cliquez sur Supprimer.

   Un message de confirmation s'affiche.
6. Cliquez sur Yes (Oui).

   Les résultats suivants se produisent :
   - Le message confirmation se ferme.
   - Le routeur est supprimé de la page Interfaces actives et cesse de consommer de la capacité.
   - Toutes les interfaces, les interfaces virtuelles personnalisées, les données (historiques) de résolution en 15 minutes et les interruptions associées sont supprimées.
   - Le routeur est supprimé de tous les cumuls associés.
   - Les données des interfaces supprimées n'apparaissent plus dans la console NFA ni dans les rapports.

Remarque : Le routeur que vous supprimez de la page Interfaces actives réapparaît sur cette page, si les interfaces de routeur sont activées sur la page Interfaces disponibles et si elles recommencent à envoyer des flux.

Voir également :

Suppression de routeurs dans le système (page 83)

Suppression d'interfaces

La suppression d'une interface sur la page Interfaces actives entraîne la suppression de ses données historiques, de ses interfaces virtuelles personnalisées et de ses interruptions. La suppression affecte également tous les cumuls, les vues et les rapports qui incluaient l'interface.

Procédez comme suit :

1. Désactivez l'interface, si elle n'est pas déjà désactivée :
   a. Ouvrez la page Interfaces disponibles :
      - Dans le menu de console NFA, sélectionnez Administration.

        La page Administration s'ouvre.
      - Dans le menu Administration, sélectionnez Système : Activer.

        La page Interfaces disponibles s'ouvre.

   b. Localisez l'interface à l'aide de la fonction de recherche ou en développant le contenu des routeurs.
   c. Cochez la case à côté de l'interface.

      Vous pouvez sélectionner et désactiver plusieurs interfaces simultanément, y compris des interfaces avec des routeurs parents différents. Toutefois, toutes vos sélections doivent être effectuées sur la même page d'affichage.
   d. Cliquez sur Désactiver.

      Le statut Activé devient Non pour l'interface. Les nouvelles données de l'interface ne sont plus collectées ni affichées dans les rapports, mais les données déjà collectées sont encore disponibles pour les rapports.
2. Ouvrez la page Interfaces actives :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.

      La page Interfaces actives s'ouvre.
3. Localisez l'interface et activez sa case à cocher.
4. Cliquez sur Supprimer.

   Un message de confirmation s'affiche pour vous prévenir des résultats de la suppression.

5. Cliquez sur Yes (Oui).

   Les résultats suivants se produisent :

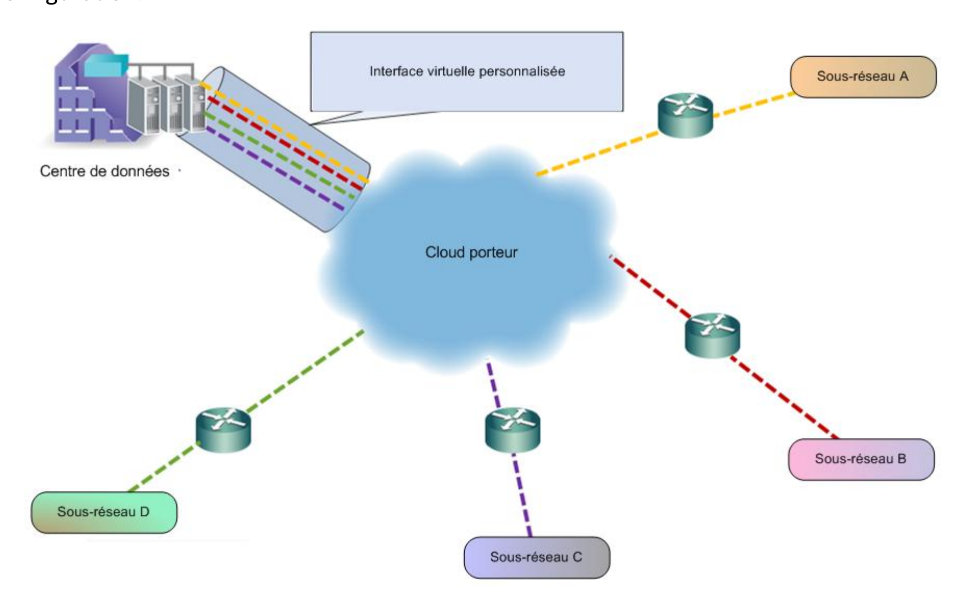
   - Le message confirmation se ferme.
   - L'interface est supprimée de la page Interfaces actives, mais pas de la page Interfaces disponibles.
   - Toutes les données d'historique associées sont purgées de façon permanente.
   - Les données de l'interface supprimée n'apparaissent plus dans les vues et les rapports de la console NFA.
   - Toutes les interfaces virtuelles personnalisées et les interruptions liées sont supprimées.
   - L'interface est supprimée de tous les cumuls associés.
   - L'interface arrête de consommer la capacité sur le serveur sur lequel sont stockées ses données.

Création d'interfaces virtuelles personnalisées

Vous pouvez créer des interfaces virtuelles personnalisées pour générer des rapports sur le trafic de sous-réseau. Créez des interfaces virtuelles personnalisées pour un réseau conçu de la façon suivante :

- Le trafic d'un centre de données est transféré aux sous-réseaux à travers un cloud porteur MPLS (Multiprotocol Label Switching).
- Le flux est activé sur les routeurs du centre de données plutôt que sur les routeurs à la périphérie du cloud.

Sans interfaces virtuelles, vous ne disposez que d'une visibilité limitée pour identifier les sous-réseaux qui génèrent le trafic pour le cloud porteur. Les interfaces virtuelles vous aident à collecter des données détaillées sur le trafic du sous-réseau dans ce type de configuration.



La définition d'une interface virtuelle personnalisée permet de distinguer le trafic correspondant à une interface du reste du trafic. L'interface virtuelle personnalisée du diagramme distingue le trafic du reste du trafic à l'entrée et à la sortie du centre de données dans le cloud.

Configuration des interfaces virtuelles personnalisées

Créez une interface virtuelle personnalisée pour distinguer le trafic dans une interface et un sous-réseau spécifiques du reste du trafic dans l'interface.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.

      La page Interfaces actives s'ouvre.

2. Développez la liste des interfaces pour le routeur parent en cliquant sur la flèche située près du nom du routeur.
3. Sélectionnez la case à cocher située près du nom d'une interface unique.
4. Cliquez sur Ajouter une interface virtuelle personnalisée.

   La boîte de dialogue Ajouter une interface virtuelle personnalisée s'ouvre.

5. Saisissez les informations pour les champs suivants :
   - Nom de l'interface : remplacez la valeur par défaut par un nom significatif pour la liste d'interfaces.

     Valeur par défaut : nom de l'interface parent, que vous devez remplacer.

   - (Facultatif) Description : entrez une chaîne de texte pour faciliter l'identification de l'interface.
   - (Facultatif) Vitesse en entrée et vitesse en sortie : identifiez la vitesse des données à l'entrée de l'interface parente et des données à la sortie de cette interface.
   - (Facultatif) Type : sélectionnez le type d'interface dans la liste.
   - Domaine : sélectionnez un domaine/client hébergé dans la liste ou acceptez le paramètre par défaut.

     La modification du domaine peut affecter le type d'opérateurs et de rapports ayant accès aux données. L'option Domaine est visible uniquement dans les environnements qui contiennent plusieurs domaines.

   - Sous-réseau : entrez une identification de sous-réseau et de masque pour chaque filtre de sous-réseau à utiliser pour l'interface virtuelle personnalisée, puis cliquez sur Ajouter. Utilisez le format suivant : <adresse_IP_sous-réseau/masque_sous-réseau>

     Les interfaces virtuelles personnalisées doivent contenir au moins un filtre de sous-réseau.

6. Cliquez sur Enregistrer.

   L'interface virtuelle personnalisée est automatiquement déployée dans la minute qui suit. L'icône de classe de la nouvelle interface virtuelle personnalisée la distingue des interfaces physiques.

Important : Si vous supprimez une interface virtuelle personnalisée parente, toutes ses interfaces virtuelles personnalisées enfants seront automatiquement supprimées.

Priorités des interfaces virtuelles personnalisées

Les priorités des interfaces virtuelles personnalisées sont définies selon le degré de spécification du masque de sous-réseau. Les masques de sous-réseau de spécificité élevée sont prioritaires. Une interface virtuelle personnalisée qui inclut un masque de sous-réseau de noeud unique (192.168.20.2/32 par exemple) a en effet priorité sur une interface virtuelle personnalisée qui inclut un masque de sous-réseau à noeuds multiples (192.0.0.0/8 par exemple). Cette méthode de définition des priorités permet de garantir la séparation du trafic de l'interface virtuelle personnalisée et du trafic de tout autre type, en particulier pour les hôtes appartenant à un sous-réseau étendu.

Remarque : Les rapports générés pour le trafic entre deux interfaces virtuelles personnalisées possédant la même priorité sont parfois incohérents.

Exemple de définitions d'interfaces virtuelles personnalisées

Si vous définissez les interfaces virtuelles personnalisées suivantes :

- CVI-A : 192.168.0.0/16
- CVI-B : 192.168.100.0/24
- CVI-C : 192.168.100.123/32

La génération de rapports suivante est activée :

- CVI-A génère un rapport sur le trafic qui implique le sous-réseau 192.168.*x*.*x*, à l'exception du trafic qui implique le sous-réseau 192.168.100.*x*.
- CVI-B génère un rapport sur le trafic qui implique le sous-réseau 192.168.100.*x*, à l'exception du trafic qui implique le sous-réseau 192.168.100.123.
- CVI-C génère un rapport sur le trafic qui implique l'hôte 192.168.100.123.

Si vous ajoutez 192.168.100.124/32 en tant que CVI-D, CVI-C ou CVI-D génère un rapport sur le trafic entre 192.168.100.123 et 192.168.100.124. Seule l'une des interfaces virtuelles personnalisées génère des rapports sur le trafic.

Si vous ajoutez 192.168.200.0/24 en tant que CVI-E, CVI-B ou CVI-E génère un rapport sur le trafic entre 192.168.100.*x* et 192.168.200.*x*. Seule l'une des interfaces virtuelles personnalisées génère des rapports sur le trafic.

Fusion d'interfaces

Vous pouvez fusionner des interfaces de manière à ce qu'elles apparaissent comme une interface unique dans les rapports. Cette opération peut s'avérer utile lorsque des modifications logiques majeures sont apportées à une unité et entraînent la création d'une interface dans le système.

A propos de la fusion des interfaces

Tenez compte des directives ci-dessous lorsque vous fusionnez des interfaces :

- Vous pouvez fusionner deux interfaces, qui peuvent se trouver sur des routeurs différents.
- La période de collecte de données relatives aux interfaces peut inclure des temps morts.
- Si vous fusionnez des interfaces dont les périodes se chevauchent, les données se chevauchant sont rejetées. La priorité est donnée à la dernière interface, c'est-à-dire à l'interface dont la date de début est la plus récente.

  Par exemple, supposons que vous fusionnez les interfaces A et B. La collecte des données sur l'interface A a lieu de 13 h 00 à 17 h 00 le même jour. La collecte des données de l'interface B commence à 15 h 00. Les données fusionnées se composent donc des données de l'interface A collectées entre 13 h 00 et 15 h 00 heures et des données de l'interface B collectées à partir de 15 h 00.
- Vous ne pouvez pas fusionner des interfaces sur lesquelles la collecte des données a débuté à la même heure.

Exemple

Par exemple, supposons que votre liaison à 512 Kbits/s a été exécutée pendant une année et est mise à niveau vers une liaison T1 (liaison à 1,54 Mbits/s). L'utilisation de la nouvelle liaison T1 entraîne la modification de l'identificateur ifIndex de l'interface. Par exemple, le numéro de l'identificateur ifIndex précédent passe de 5 à 13, l'identificateur 13 devenant le prochain identificateur ifIndex disponible pour la liaison T1. D'autres paramètres sont modifiés ou créés, notamment les paramètres ifdescr et ifAlias.

En raison de ces modifications, le programme considère l'interface comme nouvelle. Vous devez donc activer cette nouvelle interface pour que le programme puisse collecter ses données.

A ce stade, l'historique de l'interface est divisé en plusieurs fragments. Pour l'unifier, vous devez fusionner les deux versions de l'interface. Une fois la fusion terminée, l'historique inclut les données collectées préalablement à partir de l'interface sur la liaison la plus lente ainsi que les données provenant de l'interface sur la nouvelle liaison. Les données sont combinées de bout en bout sans chevauchement ni duplication.

Etapes de la fusion des interfaces

Procédez comme suit :

1. Ouvrez la page Interfaces actives :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.

      La page Interfaces actives s'ouvre.

2. Développez la liste d'interfaces pour un routeur en cliquant sur la flèche à côté du routeur.

   Une liste des interfaces pour le routeur sélectionné se développe.

3. Activez la case à cocher située à côté des deux interfaces à fusionner.

   Le bouton Fusionner situé dans la partie supérieure de la page est activé et n'est plus grisé.

   Remarque : Le bouton Fusion est activé uniquement si vous avez sélectionné deux interfaces.

4. Cliquez sur Fusionner.

   La boîte de dialogue Confirmation de la fusion des interfaces s'affiche.

5. Vérifiez que les informations de la boîte de dialogue de confirmation sont correctes :

   - Assurez-vous que l'interface affichée en tant qu'interface source (définie dans les champs sous l'étiquette Emplacement des données à copier) est bien celle dont vous voulez copier les données.
   - Vérifiez que l'interface affichée en tant qu'interface de destination (définie dans les champs sous l'étiquette Emplacement de copie des données) est bien celle vers laquelle vous voulez copier les données.
   - Cochez la case Supprimer l'interface source une fois les données fusionnées pour supprimer l'interface source automatiquement après la copie des données.

6. Cliquez sur Enregistrer.

   Les interfaces sélectionnées sont fusionnées selon les valeurs définies dans la boîte de dialogue Confirmation de la fusion des interfaces.

Personnalisation de la page

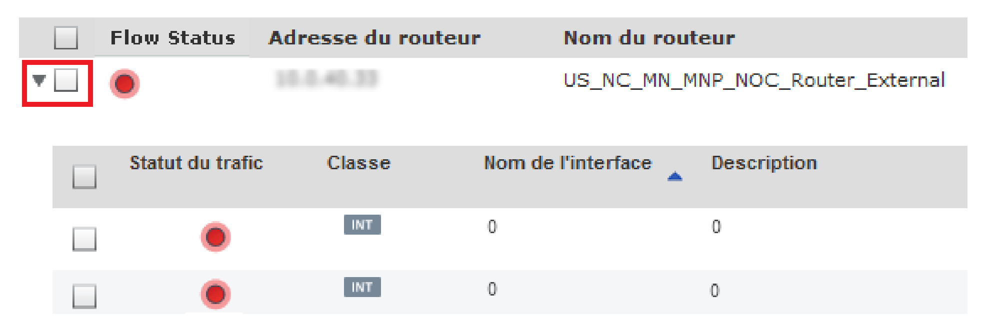
Vous pouvez personnaliser l'apparence de la page Interfaces actives pour faciliter l'accès aux informations. Vous pouvez trier les tables, afficher les détails des routeurs et modifier le nombre maximum d'interfaces et d'interfaces virtuelles personnalisées affichées dans les pages de détails sous chaque routeur.

Tri des données de table

Pour trier les données, cliquez sur un champ de menu. Par exemple, pour afficher tous les routeurs avec un indicateur de statut rouge, cliquez sur Statut du flux. Les résultats sont triés en fonction de l'horodatage correspondant au statut du flux.

Développement des détails pour les routeurs

Pour développer les détails d'un routeur, cliquez sur la flèche à gauche de la ligne du routeur. Une liste d'interfaces est affichée sous la ligne du routeur.



Remarque : Le nombre de détails affichés dans la vue développée est limité par la valeur Nombre maximum par page définie pour le routeur sélectionné.

Pour afficher ou masquer les détails de tous les routeurs, les interfaces ou les interfaces virtuelles personnalisées, cliquez sur Tout développer ou Tout réduire dans le coin supérieur droit.

Modification du nombre de détails affichés

Pour modifier le nombre d'éléments affichés, sélectionnez une valeur maximum différente à partir de la liste déroulante Nombre maximum par page. Vous pouvez modifier la valeur du paramètre Nombre maximum par page pour la liste de routeurs. Vous pouvez également définir une valeur du paramètre Nombre maximum par page Max pour la sous-liste d'interfaces et d'interfaces virtuelles personnalisées sous chaque routeur.

Page Interfaces disponibles

La page Interfaces disponibles affiche des informations concernant les routeurs et les interfaces. La liste des routeurs et des interfaces inclut les interfaces qui n'ont jamais été activées et qui n'ont jamais été la source des données collectées. Vous pouvez activer ou désactiver des interfaces, supprimer des routeurs en fin de vie et leurs interfaces ou encore réaliser des opérations de dépannage au niveau de l'interrogation.

Tâches liées aux routeurs :

- Révisez les données affichées, y compris le nombre total d'interfaces, le nombre d'interfaces activées et le profil SNMP qui a été utilisé.
- Effectuez un test d'interrogation avec le profil SNMP actuel (Test).
- Recherchez un profil SNMP (Détecter).
- Actualisez les informations d'interrogation et d'interface pour l'interrogateur (Actualiser).
- Activez ou désactivez toutes les interfaces d'un routeur.
- Supprimez un routeur en fin de vie et ses interfaces du système.

Tâches liées aux interfaces :

- Révisez les données affichées, y compris l'heure de la dernière réception d'un flux et le statut Activé ou Désactivé.
- Activez ou désactivez les interfaces une par une.

Procédez comme suit :

1. Ouvrez la page Interfaces disponibles :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Système : Activer les interfaces.

      La page Interfaces disponibles s'ouvre.
2. Utilisez les informations et les options comme suit (exemple) :
   - Activez les interfaces que vous voulez commencer à utiliser.
   - Désactivez les interfaces que vous n'utilisez pas.
   - Supprimez les routeurs que vous n'utiliserez plus.
   - Révisez les informations affichées en procédant comme décrit dans les rubriques Informations sur les routeurs (page 79) et Informations sur les interfaces (page 81).

Interfaces disponibles : informations sur les routeurs

La page Interfaces disponibles inclut les options et les informations suivantes pour les routeurs.

Tester 

Tentatives d'interrogation des interfaces du routeur à l'aide des paramètres affichés. Vous pouvez utiliser cette option dans le cadre d'un dépannage afin de tester la connectivité SNMP. Si la valeur Profil SNMP est manquante, le test échoue systématiquement.

- Test réussi : si le test réussit, cliquez sur Actualiser.
- Echec du test : si le test échoue, vous pouvez cliquer sur Détecter pour tenter de trouver un profil SNMP qui fonctionne. Vous pouvez également assigner un autre profil SNMP sur la page Interfaces actives et cliquer de nouveau sur Tester.

Détecter 

Recherche un profil SNMP à utiliser pour l'interrogation des interfaces du routeur. Vous pouvez utiliser l'option Détecter lorsque la valeur Profil SNMP est manquante et que vous ne savez pas quel profil utiliser.

- Opération réussie : si la détection réussit, cliquez sur Actualiser, puis sur Tester. Si le profil est différent du profil actuel, la valeur Profil SNMP est mise à jour.
- Echec : toutes les valeurs Profil SNMP qui ont été affichées avant la détection sont supprimées. La détection peut échouer pour plusieurs raisons : profil SNMP valide non disponible, accès bloqué au profil, routeur hors ligne, etc.

Actualiser 

Envoie les informations d'interrogation et d'interface mises à jour à l'interrogateur. Une fois l'opération Détecter ou Tester réussie, cliquez sur Actualiser.

Activer et Désactiver

Ces options permettent d'autoriser ou d'interdire l'envoi de flux à CA Network Flow Analysis par une interface (ou par le routeur et ses interfaces). Pour en savoir plus, reportez-vous à la rubrique Activation ou désactivation des interfaces (page 82).

Supprimer

Supprime le routeur et ses interfaces du système. Pour en savoir plus, reportez-vous à la rubrique Suppression de routeurs dans le système (page 83).

Options standard des pages

- Rechercher : recherche des routeurs ou des interfaces par adresse ou nom (page 65)
- Nombre maximum par page : modification du nombre d'éléments affichés (page 77)

– Développement ou réduction du contenu d'un routeur (page 77)

– Tri du contenu par colonne (page 77)

Colonnes liées aux routeurs

Statut du flux

Indicateur de statut permettant de savoir si la dernière tentative standard d'interrogation a réussi :

- Rouge : les interfaces activées n'ont pas reçu de flux pendant une durée supérieure à la **limite d'absence de données d'interface**.
- Jaune : les interfaces activées n'ont pas reçu de flux au cours de la durée comprise entre les 30 dernières minutes et la **limite d'absence de données d'interface**.
- Vert : toutes les interfaces activées ont reçu un flux au cours des 30 dernières minutes.

Adresse du routeur

Adresse IP du routeur

Nom du routeur

Nom du routeur

profil SNMP

Nom du profil SNMP utilisé lors de la dernière tentative d'interrogation réussie. Si ce profil ne fonctionne pas lors de la prochaine tentative d'interrogation, l'interrogateur utilise le profil disponible suivant autant de fois que nécessaires jusqu'à la réussite de l'interrogation. Dans ce cas, la valeur Profil SNMP est mise à jour. Si l'interrogation échoue pour tous les profils, aucune valeur n'est affichée dans le champ Profil SNMP.

Total d'interfaces

Nombre total d'interfaces du routeur

Interfaces activées

Nombre total d'interfaces activées pour le routeur

Harvester

Adresse IP du Harvester parent du routeur

Interfaces disponibles : informations sur les interfaces

La page Interfaces disponibles inclut les options et les informations suivantes pour les interfaces.

Activer et Désactiver

Ces options permettent d'autoriser ou d'interdire l'envoi de flux au produit par une interface (ou par le routeur et ses interfaces). Pour en savoir plus, reportez-vous à la rubrique Activation ou désactivation des interfaces (page 82).

Options standard des pages : options standard des pages décrites dans la rubrique Interfaces disponibles : informations sur les routeurs (page 79)

Colonnes liées aux interfaces

Les valeurs ifName, ifAlias, Nom du port et vrfName sont présentes uniquement si le routeur parent est configuré pour fournir ces informations à l'interrogateur. Ces informations proviennent de la base de données d'interfaces. Les modifications que vous avez éventuellement apportées aux propriétés correspondantes sur la page Interfaces actives ne sont pas reflétées ici.

Activé

Autorise l'interface à envoyer des flux au produit (Oui) ou l'interdit d'envoyer des flux (Non).

License

Statut indiquant si l'interface a envoyé un flux au produit (Oui) ou si elle n'a jamais envoyé de flux (Non). Si la valeur est Non, le système n'inclut pas d'enregistrements pour l'interface.

ifIndex

Valeur d'index d'identification assignée automatiquement à l'interface

ifName

Nom de l'interface

ifAlias

Alias de l'interface

Nom du port

Nom du port de l'interface

vrfName

Nom de routage et de transfert virtuel

Vitesse

Vitesse maximum de transmission des données pour l'interface

Dernier flux

Date et heure du dernier traitement du flux. Si une collecte de flux est en cours, la valeur Dernier flux est mise à jour toutes les 15 minutes.

Activation ou désactivation des interfaces

Par défaut, les interfaces sont activées sur la page Paramètres de l'application. Vous pouvez, dans certains cas, activer les interfaces manuellement, par exemple dans les scénarios suivants :

- Les interfaces ont été désactivées temporairement et vous voulez les réactiver.
- Le programme n'est pas configuré pour activer automatiquement les interfaces nouvellement détectées. L'option Activer les interfaces automatiquement de la page Paramètres de l'application est définie sur False.

L'activation d'une interface déclenche instantanément les événements suivants :

- Vous pouvez utiliser l'interface comme filtre dans les rapports d'examen des flux.

  Parmi les données disponibles dans les rapports d'examen des flux figurent les données collectées pendant la durée de la désactivation de l'interface.
- D'autres types de données d'interface sont collectées et stockées, notamment les données relatives aux hôtes, aux conversations, aux types de service et aux prototypes. Une fois la période initiale de collecte des données terminée, vous pouvez afficher les données d'interface supplémentaires dans les rapports d'interface d'analyse en profondeur, dans les rapports d'analyse et dans les rapports personnalisés.

Procédez comme suit :

1. Ouvrez la page Interfaces disponibles :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Système : Activer les interfaces.

      La page Interfaces disponibles s'ouvre.
2. Cliquez sur la flèche à côté du routeur qui contient les interfaces.

   La vue s'étend pour indiquer la liste des interfaces. La colonne de statut Activé indique les interfaces activées.
3. Cochez la case à côté d'une ou de plusieurs interfaces.

4. Sélectionnez l'une des options suivantes :
   - Activer (activer la collecte des données pour l'interface)
   - Désactiver (empêcher la collecte des données pour l'interface)

   L'activation ou la désactivation de la collecte des données pour les interfaces sélectionnées est immédiate.

Suppression de routeurs dans le système

Si vous supprimez un routeur dans la page Interfaces disponibles, ce routeur est supprimé du système de façon permanente. Cette opération supprime le routeur, ses information de configuration, les données (historiques) de résolution en 15 minutes, les interfaces, les interfaces virtuelles personnalisées et les interruptions. La suppression s'applique également à l'ensemble des agrégations, des vues et des rapports dans lesquels l'interface était incluse.

Remarque : Si les interfaces du routeur supprimé recommencent à envoyer des flux, un nouveau routeur s'affiche sur la page Interfaces disponibles. Si le programme est configuré pour activer les nouvelles interfaces de manière automatique, le nouveau routeur et les nouvelles interfaces apparaissent également sur la page Interfaces actives. Le nouveau routeur hérite du paramètre de domaine de client hébergé actuel de son Harvester parent. Les paramètres de configuration du routeur précédent sont perdus. Si CA Performance Center est inclus dans votre déploiement, le routeur utilise les profils SNMP assignés au client hébergé du Harvester pour les interrogations.

Procédez comme suit :

1. Vérifiez que le routeur n'envoie plus de flux à CA Network Flow Analysis.
2. Ouvrez la page Interfaces disponibles :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Système : Activer les interfaces.

      La page Interfaces disponibles s'ouvre.
3. Localisez le routeur et activez sa case à cocher.
4. Cliquez sur Supprimer.

   Un message de confirmation s'affiche.
5. Cliquez sur Yes (Oui).

   Les résultats suivants se produisent :
   - Le message confirmation se ferme.
   - Le routeur est supprimé du système, de la page Interfaces disponibles et de la page Interfaces actives.

- Les informations de configuration du routeur sont supprimées du serveur de la console NFA.
- Toutes les interfaces, les interfaces virtuelles personnalisées, les données (historiques) de résolution en 15 minutes et les interruptions associées sont supprimées.
- Le routeur est supprimé de tous les cumuls associés.
- Les données des interfaces supprimées n'apparaissent plus dans la console NFA ni dans les rapports.

Définition des modèles de nom d'interface

Pour modifier les règles qui déterminent l'affichage des noms et des descriptions d'interface dans la console NFA, utilisez l'une des procédures suivantes :

- Créez un modèle d'interface et définissez-le en tant que modèle actif pour CA Network Flow Analysis.
- Modifiez le modèle d'interface actuel.
- Affinez l'attribution des noms d'interfaces pour des vues de console NFA spécifiques à l'aide de la page Paramètres de l'application.

Vous pouvez créer plusieurs modèles d'interface, mais seul le modèle d'interface actuellement sélectionné déterminera les noms et les descriptions d'interfaces dans la console NFA, dans ses vues et dans ses rapports imprimés.

(CA PC uniquement) Le modèle d'interface actuellement sélectionné affecte également les noms et descriptions d'interface dans certaines vues CA Performance Center des données CA Network Flow Analysis. Les emplacements suivants dans CA Performance Center peuvent afficher des noms et des descriptions d'interface différents : pages d'interface (onglet Détails), pages d'inventaire et vues de tendance. Pour personnaliser les descriptions d'interface dans CA Performance Center, appliquez des substitutions de descriptions d'interface à des domaines spécifiques.

Création et application d'un modèle d'interface personnalisé

Créez un modèle d'interface personnalisé pour modifier l'affichage des noms d'interface et des descriptions dans la console NFA.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Affichez la page Modèles d'interface dans la console NFA :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Système : Modèles.

      La page Modèles d'interface s'ouvre.
3. Cliquez sur Ajouter.

   La page Modèles d'interface affiche les options d'ajout de modèle d'interface.
4. Spécifiez les paramètres de modèle d'interface :
   - Nom : texte d'identification affiché dans la liste des modèles.
   - Nom d'interface : propriétés, texte ou propriétés et texte qui constituent le nom de chaque interface dans la console NFA.
   - Description de l'interface : propriétés, texte ou propriétés et texte qui constituent la description de chaque interface dans la console NFA.

   Utilisez les propriétés de la liste suivante pour les deux paramètres :
   - *[Alias de l'unité] :* nom d'unité (routeur) affiché dans la console NFA.
   - *[Nom de l'unité] :* nom DNS ou adresse IP de l'unité (routeur).
   - *[ifDescr] :* description de l'interface provenant de la valeur ifDescr d'origine dans la table ifEntry SNMP (sauf si la description d'interface a été personnalisée). Si la description d'interface a été personnalisée sur la page Interfaces actives, la valeur personnalisée est utilisée.
   - *[ifAlias] :* alias de l'interface
   - *[ifName] :* nom de l'interface provenant de la valeur ifName d'origine dans la table ifEntry SNMP (sauf si le nom d'interface a été personnalisé). Si le nom de l'interface a été personnalisé sur la page Interfaces actives, la valeur personnalisée est utilisée.
   - *[Nom du port] :* nom du port, qui peut être le numéro de port.
   - *[ifIndex] :* identificateur numérique unique pour l'interface tel que défini dans la table ifEntry SNMP
   - *[ifType] :* type d'interface, tel que défini dans le champ ifType de la table SNMP ifEntry.
5. Cliquez sur Soumettre.

   Le nouveau modèle est créé et ajouté à la liste de modèles. Les options supplémentaires sont supprimées de la page Modèles d'interface.

6. (Facultatif) Appliquez le modèle : sélectionnez le modèle dans la liste au haut de la page Modèles d'interface.

   Le modèle est appliqué à la console NFA presque immédiatement. Les vues Performance Center qui utilisent le modèle reflètent les modifications apportées lors de la prochaine synchronisation, qui est lancé dans les 5 minutes suivantes.

7. (Facultatif) Révisez le modèle modifié. Par exemple, révisez les nouvelles étiquettes sur les pages Interface et Présentation de l'entreprise.

Conventions des modèles d'interface

Les paramètres de modèle d'interface comprennent des propriétés, du texte brut ou des propriétés et du texte brut. Les conventions suivantes s'appliquent aux modèles d'interface :

- Entourez les propriétés de crochets.
- Séparez les différentes propriétés d'une barre verticale. La première propriété qui renvoie une valeur est affichée. Spécifiez suffisamment de propriétés pour pouvoir tenir compte des interfaces pour lesquelles des définitions de propriété sont manquantes.
- Pour afficher les noms d'interface ou les descriptions en texte brut, incluez le texte sans utiliser de parenthèses.

Modification d'un modèle d'interface

Modifiez un modèle d'interface pour modifier l'affichage des noms d'interface et des descriptions dans la console NFA lorsque le modèle est sélectionné.

Procédez comme suit :

1. Affichez la page Modèles d'interface dans la console NFA :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Système : Modèles.

      La page Modèles d'interface s'ouvre.

2. Sélectionnez le modèle dans la liste en haut de la page.

3. Cliquez sur Modifier.

   Un message de confirmation s'affiche.

4. Cliquez sur OK.

   Le contenu des champs Nom de l'interface et Description de l'interface est modifiable.

5. Spécifiez les paramètres de modèle d'interface :
   - Nom de l'interface : texte et/ou propriétés qui constituent le nom des interfaces dans la console NFA.
   - Description de l'interface : texte et/ou propriétés qui constituent la description des interfaces dans la console NFA.

   Définissez les deux paramètres avec les propriétés de la liste dans la rubrique sur la création d'un modèle (page 84):
6. Cliquez sur Mettre à jour.

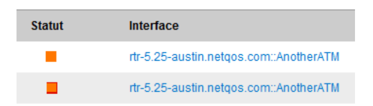
   Le contenu des champs est mis à jour et n'est plus modifiable.

   Les noms d'interface et les définitions sont affichés dans la console NFA presque immédiatement. Les vues CA Performance Center qui utilisent le modèle affichent les modifications lors de la prochaine synchronisation, qui a automatiquement lieu dans un délai de 5 minutes.
7. (Facultatif) Révisez le modèle modifié. Par exemple, révisez les nouvelles étiquettes sur les pages Interface et Présentation de l'entreprise.

Modification du paramètre de l'application pour les noms d'interface

Pour changer la convention d'attribution des noms des interfaces, vous pouvez utiliser un paramètre de la page Paramètres de l'application. Le paramètre par défaut ajoute le nom de l'unité avant le nom de l'interface. Ce paramètre affecte la manière dont les noms d'interface s'affichent dans certaines vues de rapport de console NFA, telles que les vues de présentation de l'entreprise, les pages d'interfaces et les récapitulatifs d'interfaces des rapports personnalisés.

Les noms d'interface obtenus peuvent inclure des doublons superflus. Par exemple, si une unité et une interface sont toutes les deux nommées Device1, le nom d'interface Device1::Device1 est affiché par défaut. L'exemple suivant illustre cette répétition.



Statut	Interface
	rtr-5.25-austin.netqos.com::AnotherATM
	rtr-5.25-austin.netqos.com::AnotherATM

Pour éliminer cette duplication, dans la page Paramètres de l'application, modifiez le paramètre Afficher le nom de l'unité.

Procédez comme suit :

1. Affichez la page Paramètres de l'application :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Système : Paramètres de l'application.

      La page Paramètres de l'application s'affiche.

2. Définissez la valeur de l'option Afficher le nom de l'unité sur False.

3. Cliquez sur Enregistrer.

   Lorsque la valeur de Afficher le nom de l'unité est False, les noms des unités dans les rapports et les vues ne sont pas ajoutés aux noms d'interfaces.

Chapitre 5: Utilisation des groupes et des agrégations d'interfaces

Les options de création et de gestion des groupes d'interfaces sont disponibles dans Performance Center dès l'enregistrement du produit comme source de données (page 15). Les groupes d'interfaces personnalisés permettent aux utilisateurs d'optimiser les résultats des rapports et des analyses personnalisés. Par exemple, les groupes d'interfaces peuvent aider les opérateurs à configurer des rapports personnalisés basés sur l'emplacement géographique, la vitesse d'interface, les sites T1 ou l'équilibrage de la charge.

Vous pouvez créer et gérer des cumuls d'interface à partir de la console NFA. Un cumul d'interface associe le trafic provenant de plusieurs interfaces de telle façon que les rapports sont générés pour un trafic unifié. Supposons par exemple que vous avez deux circuits à charge équilibrée et que vous voulez générer un rapport global unique sur leurs interfaces. Les agrégations vous permettent de générer un rapport unique sur les interfaces, sans devoir configurer un rapport personnalisé à cet effet. Tous les cumuls s'affichent dans l'index d'interface sous l'étiquette *Cumuls*.

Remarque : Vous pouvez cumuler des interfaces uniquement lorsque leurs données sont collectées par le même composant de collecte. Ne cumulez aucune interface à partir de plusieurs composants de collecte.

Création d'agrégations d'interface

Créer des agrégations d'interface pour associer le trafic provenant de plusieurs interfaces de telle façon que les rapports sont générés pour un trafic unifié.

Par exemple, vous créez des agrégations pour chaque région géographique. Les opérateurs utilisent les agrégations dans des rapports pour vérifier et comparer les totaux de ces régions. Avant la création d'agrégations, les opérateurs rencontraient les problèmes suivants :

- Les données étaient clairsemées sur plusieurs rapports.
- Les valeurs n'étaient pas cumulées par région ; les synthèses et les comparaisons rapides étaient donc difficiles à effectuer.
- Les opérateurs passaient trop de temps à concevoir des rapports spécialisés pour la collecte de données et la création des totaux dont ils avaient besoin.

Procédez comme suit :

1. Affichez la page Agrégations d'interfaces :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Interfaces : Agrégations.

      La page Agrégations d'interfaces s'ouvre et affiche la liste des agrégations d'interfaces actuelles.

2. Cliquez sur Créer.

   La page est actualisée pour afficher les options permettant l'ajout d'une agrégation.

   Sélectionnez les interfaces à ajouter à l'agrégation à l'aide de l'une des méthodes suivantes :

   - *Sélection de routeurs :* cochez les cases à côté d'un ou de plusieurs noms de routeur. Vous pouvez sélectionner un ou plusieurs routeurs, ou une combinaison de routeurs et d'interfaces individuelles pour un routeur qui n'est pas sélectionné. Lorsqu'un routeur a été sélectionné, aucune de ses interfaces individuelles ne peut être sélectionnée.
   - *Sélection d'interfaces :* cliquez sur Tout développer ou cliquer sur la flèche à côté d'un nom de routeur, puis sélectionnez les interfaces dans la liste. Pour sélectionner toutes les interfaces d'un routeur, cochez la case de la ligne de titre.
   - *Filtrage de la liste pour rechercher des routeurs ou des interfaces :* pour filtrer l'affichage, saisissez une chaîne de texte dans la zone de recherche, puis cliquez sur Rechercher. Vous pouvez rechercher un nom complet, un nom partiel, l'adresse d'un routeur ou l'adresse d'une interface. La liste des routeurs/interfaces est filtrée pour afficher les routeurs correspondants ou les routeurs qui contiennent des interfaces correspondantes.

- *Filtrage de la liste pour vérifier les sélections :* cliquez sur Afficher la sélection pour afficher uniquement les routeurs sélectionnés ou qui contiennent les interfaces sélectionnées. Vous pouvez associer cette fonction à une chaîne de recherche et utiliser l'option Tout développer pour localiser et vérifier rapidement vos sélections.

3. Spécifiez les valeurs suivantes, puis cliquez sur Enregistrer :

   - Routeurs et/ou Interfaces : sélectionnez un ou plusieurs routeurs ou interfaces répertoriés au bas de la page. Vos sélections sont ajoutées à l'agrégation.
   - Nom de l'agrégation : spécifiez un nom pour l'agrégation.
   - Description (facultatif) : ajoutez une note pour faciliter l'identification de l'agrégation.
   - Vitesse d'entrée (facultatif) : spécifiez la vitesse d'entrée des interfaces sélectionnées.
   - Vitesse de sortie (facultatif) : spécifiez la vitesse de sortie des interfaces sélectionnées.

     Si vous ne spécifiez aucune vitesse d'entrée et de sortie, les valeurs sont définies sur 0 par défaut. Les vitesses inexactes rendent certains résultats de rapport inexacts, notamment les pourcentages d'utilisation.
   - Type (facultatif) : sélectionnez le mode de connexion de l'interface dans la liste Type, comme WAN ou Ethernet.

     Si vous ne spécifiez aucun type d'interface, le type est défini sur Inconnu par défaut.

   L'agrégation est automatiquement déployée en quelques minutes.

Modification des agrégations d'interfaces

Modifiez une agrégation d'interface pour sélectionner différentes interfaces à agréger ou pour modifier le nom de l'agrégation, la description, la vitesse ou le type d'interface.

Procédez comme suit :

1. Affichez la page Interfaces d'agrégation :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Interfaces : Agrégations.

      La page Agrégations d'interfaces s'ouvre et affiche la liste des agrégations d'interfaces actuelles.

2. Cochez la case à côté de l'agrégation que vous voulez modifier, puis cliquez sur Modifier.

   La page passe en mode Modifier une agrégation et les options de modification sont disponibles.

3. Apportez les modifications nécessaires : ajoutez ou supprimez des interfaces, ou modifiez le nom de l'agrégation, la description, la vitesse d'entrée/de sortie ou le type.

4. Cliquez sur Enregistrer.

   Vos modifications sont enregistrées et vous revenez à la liste des agrégations.

Suppression de cumuls d'interface

Supprimez les cumuls d'interface dont vous n'avez plus besoin.

Procédez comme suit :

1. Affichez la page Agrégations d'interfaces :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Interfaces : Agrégations.

      La page Agrégations d'interfaces s'ouvre et affiche la liste des agrégations actuelles.

2. Cochez la case située à côté de chaque cumul à supprimer.

3. Cliquez sur Supprimer.

4. Dans le message de confirmation qui s'affiche, cliquez sur Oui.

   Tous les cumuls sélectionnés sont supprimés automatiquement.

Chapitre 6: Utilisation des Harvesters et des DSA

Cette section décrit les tâches associées aux Harvesters et aux DSA (dans un déploiement à trois niveaux).

Utilisez la page Harvester pour effectuer les opérations suivantes :

- Ajout et suppression de Harvesters (page 93)
- Modification des détails d'un Harvester (page 94)

Si vous travaillez dans un déploiement à trois niveaux, utilisez la page DSA pour effectuer les opérations suivantes :

- Ajout et suppression de DSA (page 33)
- Modification de l'adresse IP d'un DSA actuel (page 97) ou d'un nouveau DSA (page 98)

Ajout et suppression de Harvesters

Ajoutez et supprimez des Harvesters à partir de la page Harvester.

Pour ajouter un Harvester, effectuez les opérations de la rubrique Ajout d'un Harvester (page 28).

Pour supprimer un Harvester, effectuez les opérations décrites dans cette rubrique.

Remarque : Si vous supprimez un Harvester, vous devez réimager le serveur d'installation et réinstaller le logiciel de Harvester pour pouvoir ajouter l'instance de ce même Harvester. Une fois que vous avez supprimé un Harvester, vous ne pouvez plus récupérer les données déjà collectées.

Procédez comme suit :

1. Ouvrez la page Harvester.
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu de la page Administration, sélectionnez Système : Harvester.

      La page Harvester s'ouvre et affiche un tableau contenant les informations sur les Harvesters connus.

2. Dans la ligne du Harvester que vous souhaitez supprimer, cliquez sur Supprimer.

   Un message de confirmation s'affiche.

3. Cliquez sur Oui pour confirmer la suppression du Harvester.

   Le Harvester est supprimé et n'est plus répertorié dans le tableau Harvester. La console NFA ne collecte plus les données des routeurs associés au Harvester supprimé. Les données de ces routeurs qui ont été collectées précédemment ne sont plus disponibles dans les rapports.

Modification des détails de Harvester

Modifiez les détails des Harvesters à partir de la page Harvester. Vous pouvez modifier l'adresse IP, la description et le paramètre client hébergé/domaine.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.

   La page Administration s'ouvre.

2. Dans le menu de la page Administration, sélectionnez Système : Harvester.

   La page Harvester s'ouvre et affiche un tableau contenant les informations concernant les Harvesters connus.

3. Sur la ligne Harvester que vous souhaitez modifier, cliquez sur Modifier.

   La boîte de dialogue Modifier le Harvester s'ouvre.

4. (Facultatif) Modifiez les paramètres suivants si nécessaire :

   Adresse IP

   Adresse IP du Harvester.

   Description

   (Facultatif) Informations supplémentaires permettant d'identifier le Harvester.

Domaine

Combinaison client hébergé/domaine du Harvester dans un déploiement à domaines multiples.

La modification de ce paramètre affecte la combinaison client hébergé/domaine pour tous les nouveaux routeurs qui lancent l'exportation des données de flux. Les routeurs et les interfaces qui existent déjà conservent leurs combinaisons client hébergé/domaine précédentes.

Le domaine affecte les opérateurs et les rapports qui ont accès aux données générées par les routeurs et par les interfaces.

La modification du client hébergé d'un routeur dans CA Performance Center peut affecter les profils SNMP disponibles pour l'interrogation. Cette limitation n'est pas applicable à CA NetQoS Performance Center, qui utilise la même liste de profils SNMP pour tous les routeurs.

Valeur par défaut : Client hébergé par défaut\Domaine par défaut.

Si aucun domaine IP personnalisé n'a été créé, la table Harvester inclut uniquement les colonnes Adresse IP et Description.

5. Cliquez sur Enregistrer.

   Vos modifications sont enregistrées immédiatement et apparaissent dans le tableau Harvester.

Modification d'adresses IP de DSA

Applicable à : une architecture à trois niveau dans un déploiement distribué (console NFA, Harvester et DSA installés sur des serveurs distincts)

Modifiez le paramètre d'adresse IP pour un DSA lorsque :

- Vous modifiez l'adresse IP d'un DSA actuel (DSA déjà en cours d'utilisation et non déplacé vers un autre serveur).
- Vous utilisez pour la première fois une DSA sur un nouveau serveur au lieu d'un DSA retiré.

  Vous modifiez l'adresse IP de l'appliance de stockage des données retirée plutôt que d'ajouter une nouvelle instance de DSA. Sinon, les routeurs continuent d'envoyer des données au DSA retiré (et ces données n'apparaissent pas dans les rapports).

Remarques : Ces tâches s'appliquent uniquement dans les cas suivants.

- Déploiements distribué de CA Network Flow Analysis à trois niveaux. Si vous disposez d'un système autonome ou d'une architecture à deux niveaux, vous n'avez pas besoin de définir ou de mettre à jour les adresses IP du DSA.
- Serveurs Windows. CA Network Flow Analysis prend en charge les DSA sur les serveurs Windows uniquement.
- Serveurs incluant des adresses IP statiques et qui ne sont pas configurés pour utiliser le protocole DHCP (Dynamic Host Configuration Protocol).

Modification de l'adresse IP d'un DSA actuellement connectée

Modifiez le paramètre d'adresse IP du DSA en cas de modification de l'adresse IP d'un DSA actuellement connecté.

Effectuez cette tâche lorsque l'adresse IP change sur un serveur de DSA. Si vous déplacez le DSA vers un nouveau serveur, ignorez cette étape et consultez la rubrique Modification de l'adresse IP d'un nouveau DSA (page 98).

Procédez comme suit :

1. Connectez-vous avec un compte disposant des droits d'administrateur de CA Network Flow Analysis.
2. Interrompez la collecte de données du DSA actuel :
   a. Ouvrez la fenêtre Services Windows sur le serveur de DSA.
   b. Sélectionnez le service de pompage de NetQoS Reporter Analyzer dans la liste Services.
   c. Cliquez sur le lien Arrêter à gauche.

      L'exécution du service s'arrête.
3. Attendez que le DSA termine le traitement des fichiers .rpr dans le répertoire suivant : <chemin_installation>/Netflow/datafiles/loaderInput.

   Cette étape permet au DSA de récupérer les données brutes qui ont été générées lors de l'arrêt du service. Le traitement prend environ 15 minutes. Le traitement se termine lorsqu'il ne reste plus de fichiers .rpr dans le répertoire loaderInput.
4. Changez l'adresse IP sur le serveur de DSA. Pour plus d'informations sur cette étape, consultez les recommandations sur le site microsoft.com.
5. Mettez à jour les paramètres de pare-feu si nécessaire.
6. Affichez la page DSA dans l'interface utilisateur de la console NFA :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Système : DSA.

      La page DSA s'ouvre et affiche la liste des DSA utilisés.
7. Dans la ligne du DSA que vous souhaitez modifier, cliquez sur Modifier.

   La boîte de dialogue Modifier le DSA s'affiche.
8. Remplacez la valeur du champ Adresse IP par l'adresse IP du nouveau serveur de DSA.
9. Cliquez sur Tester la connexion.

   Si la connexion réussit, le message Test réussi s'affiche.

10. Cliquez sur OK dans la zone de message Test réussi.

    Le message se ferme.

11. Cliquez sur Enregistrer dans la boîte de dialogue Modifier le DSA.

    La nouvelle adresse IP du DSA est enregistrée. CA Network Flow Analysis commence à utiliser la nouvelle adresse IP dès qu'il commence à stocker et à récupérer des données.

12. Redémarrez le service de pompage de NetQoS Reporter Analyzer dans la fenêtre Services Windows sur le serveur de DSA.

    Le DSA commence de nouveau à collecter des données. Il doit pouvoir récupérer toutes les données générées pendant la période d'arrêt du service.

Modification de l'adresse IP d'un nouveau DSA

Modifiez l'adresse IP du DSA pour commencer à utiliser un nouveau DSA au lieu du DSA retirée.

Effectuez cette tâche pour déplacer le DSA vers un nouveau serveur. Par exemple, en cas d'échec du serveur de DSA ou pour améliorer les performances ou l'espace de stockage. Une fois que vous remplacez l'adresse IP par l'adresse du nouveau serveur, la permutation vers le nouveau DSA est terminée.

Remarques :

- Si vous déplacez un DSA vers un nouveau serveur, les données du DSA antérieur ne sont plus disponibles dans les rapports.
- Si vous ajoutez une instance de DSA au lieu de modifier l'adresse IP d'un DSA retiré, le DSA retiré apparaît encore dans la liste. Les routeurs répartissent les données entre tous les DSA de la liste, c'est pourquoi les routeurs continuent d'envoyer des données au DSA retiré. Les rapports n'incluent pas les données qui sont envoyées vers des DSA non fonctionnels. Pour corriger ce problème, contactez le service de support de CA pour obtenir de l'aide pour la suppression du DSA obsolète.
- Si le DSA se trouve toujours sur le même serveur, ignorez cette tâche et consultez la rubrique Modification de l'adresse IP d'un DSA actuellement connecté (page 97).

Procédez comme suit :

1. Installez le logiciel de DSA sur le nouveau serveur et terminez la configuration (y compris les mises à jour de pare-feu). Pour plus d'informations sur cette étape, consultez le *Manuel d'installation de CA Network Flow Analysis*.
2. Connectez-vous à la console NFA avec un compte disposant des droits d'administrateur de CA Network Flow Analysis.
3. Exécutez et enregistrez les copies des rapports que vous voulez utiliser pour les informations d'archivage du DSA précédent.

4. Affichez la page DSA dans l'interface utilisateur de la console NFA :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Système : DSA.

      La page DSA s'ouvre et affiche la liste des DSA utilisés.
5. Dans la ligne du DSA que vous allez remplacer, cliquez sur Modifier.

   La boîte de dialogue Modifier le DSA s'affiche.
6. Remplacez la valeur du champ Adresse IP par l'adresse IP du nouveau serveur de DSA.
7. Cliquez sur Tester la connexion.

   Si la connexion réussit, le message Test réussi s'affiche.
8. Cliquez sur OK dans la zone de message Test réussi.

   Le message se ferme.
9. Cliquez sur Enregistrer dans la boîte de dialogue Modifier le DSA.

   La nouvelle adresse IP du DSA est enregistrée. Le nouveau DSA commence à collecter, à traiter et à stocker les données. Les données du DSA retiré ne sont plus disponibles dans les rapports.

Chapitre 7: Création de noms et de groupes pour les protocoles, les types de service et les données des systèmes autonomes

Cette section décrit la procédure à suivre pour créer et pour gérer des groupes de protocoles, des étiquettes de type de service, des groupes de types de service et des noms personnalisés de systèmes autonome. Ces opérations s'effectuent dans plusieurs pages différentes.

Page Configuration du groupe de protocoles

Vous pouvez utiliser la page Configuration du groupe de protocoles pour afficher les groupes de protocoles existants et leur contenu. Vous pouvez ajouter, modifier et supprimer des groupes personnalisés de protocoles.

Dans la page Administration, sélectionnez Groupes : Groupes de protocoles, puis, dans la page Configuration du groupe de protocoles, effectuez les principales opérations suivantes :

- Création d'un groupe de protocoles de shell (page 103)
- Configuration du groupe de protocoles (page 104)
- Révision et modification du groupe (page 105)

Page Configuration du type de service

Vous pouvez utiliser la page Configuration du type de service pour afficher et pour modifier les étiquettes et les descriptions des valeurs de type de service.

Dans la page Administration, sélectionnez Définir une application : Noms des types de service, puis, dans la page Configuration du type de service, effectuez l'opération suivante :

- Etiquetage des valeurs de type de service (page 107)

Page Configuration du groupe de types de service

Vous pouvez utiliser la page Configuration du groupe de types de service pour afficher les groupes de types de service existants et leur contenu. Vous pouvez ajouter, modifier et supprimer des groupes personnalisés de types de service.

Dans la page Administration, sélectionnez Groupes : Groupes de types de service, puis, dans la page Configuration du groupe de types de service, effectuez les principales opérations suivantes :

- Création d'un groupe de types de services de shell (page 108)
- Configuration du groupe de types de services (page 109)
- Modification des groupes de types de service (page 110)
- Suppression des groupes de types de service (page 111)

Page Noms des systèmes autonomes

Vous pouvez utiliser la page Noms des systèmes autonomes pour afficher et pour modifier le nom des systèmes autonomes.

Dans la page Administration, sélectionnez Groupes : Noms des systèmes autonomes, puis, dans la page Noms des systèmes autonomes, effectuez les principales opérations suivantes :

- Révision des noms des systèmes autonomes (page 113)
- Modification des noms des systèmes autonomes (page 114)

Création de groupes de protocoles

Vous pouvez utiliser les groupes de protocoles pour filtrer des données dans les rapports personnalisés et d'analyse. En tant qu'administrateur, vous pouvez configurer des groupes personnalisés de protocoles contenant des protocoles pour des types particuliers de trafic réseau.

Par exemple, si les opérateurs veulent créer des rapport sur le trafic réseau pour différents types d'applications, telles que la messagerie, la vidéoconférence, la voix sur IP et les médias de diffusion en continu. Aucun groupe de protocoles par défaut n'étant défini à cette fin, vous devez créer un groupe personnalisé de protocoles pour chaque type d'application. Chaque groupe de protocoles inclut toutes les valeurs de protocole utilisées au sein de votre entreprise pour les applications cibles.

L'utilisation d'un groupe personnalisé de protocoles ne requiert pas de connaissances approfondies sur l'utilisation de chaque protocole de la part des opérateurs, ni l'ajout de filtres individuels de protocole aux définitions de rapport.

Les rubriques suivantes indiquent aux administrateurs de CA Network Flow Analysis comment créer un groupe de protocoles de shell, configurer le groupe de protocoles, et ensuite réviser et modifier les paramètres du groupe de protocoles.

Création d'un groupe de protocoles de shell

Vous pouvez créer et configurer un groupe de protocoles de shell pour filtrer les rapports sur un type particulier de trafic réseau.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Ouvrez la page Configuration du groupe de protocoles :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Groupes : Groupes de protocoles.

      La page Configuration du groupe de protocoles s'ouvre et affiche des informations sur le groupe de protocoles actuellement sélectionné.
3. Cliquez sur Ajouter.

   Les options permettant d'identifier un nouveau groupe de protocoles apparaissent dans la page Configuration du groupe de protocoles.

4. Entrez les valeurs dans les zones Nom du groupe et Description.

   Le nom et la description s'affichent aux emplacements suivants dans CA Network Flow Analysis :

   - Liste des groupes de protocoles sur la page Configuration du groupe de protocoles
   - Index des groupes de protocoles qu'un opérateur peut afficher dans l'assistant de création de rapports pour définir un rapport d'analyse ou personnalisé

   Un nouveau groupe de protocoles de shell est créé. Le nouveau nom de groupes de protocoles est ajouté à la liste des groupes de protocoles sur la page Configuration du groupe de protocoles.

   Etape suivante : configurez le groupe de protocoles de shell.

Configuration du groupe de protocoles

Une fois que vous avez créé un groupe de protocoles de shell, l'étape suivante consiste à le configurer afin qu'il représente un type particulier de trafic réseau.

Procédez comme suit :

1. Dans la page Configuration du groupe de protocoles, sélectionnez le groupe de protocoles dans la liste Groupe de protocoles.
2. Cliquez sur Liste.

   Les options de configuration sont ajoutées à la page Configuration du groupe de protocoles.

3. (Facultatif) Révisez et corrigez le paramètre Domaine si nécessaire.

   Le paramètre Domaine s'affiche uniquement pour les environnements contenant plusieurs domaines.

   Le contenu du groupe de protocoles sélectionné affiche les noms des protocoles du domaine sélectionné. Si un administrateur a défini des noms de protocole spécifiques au domaine, la sélection de ce domaine affiche les noms de protocole correspondants.

   Le paramètre Domaine ne limite pas l'accès au groupe de protocoles ou aux rapports qui utilisent le groupe de protocoles comme filtre.

4. Sélectionnez les protocoles pour le groupe :

   a. Cliquez sur Ajouter/supprimer.

      Une boîte de dialogue s'ouvre. Elle contient la liste des protocoles disponibles et une liste des protocoles actuellement inclus dans la liste.

      Si le lien Ajouter/Supprimer n'est pas visible, cliquez sur Liste.

b. Dans le volet supérieur, sélectionnez les protocoles que vous voulez ajouter au groupe.

   Pour sélectionner plusieurs protocoles à ajouter simultanément, utilisez les touches Majuscule et Contrôle.

   Pour filtrer la liste de protocoles, saisissez une chaîne de recherche dans le champ Filtrer la liste de protocoles, puis cliquez sur Appliquer. Par exemple, pour afficher uniquement les protocoles UDP, entrez **udp**.

c. Cliquez sur Ajouter.

   Les protocoles sélectionnés sont ajoutés à la liste de protocoles.

d. Dans le volet inférieur, sélectionnez les protocoles que vous voulez supprimer du groupe.

e. Cliquez sur Supprimer.

   Les protocoles sélectionnés sont supprimés de la liste de protocoles.

f. Cliquez sur Terminé lorsque vous avez terminé de configurer le contenu du groupe de protocoles.

   Pour réviser une liste de groupes de protocoles contenant un protocole particulier, sélectionnez le protocole et cliquez sur Accéder au protocole. La page Configuration du protocole s'ouvre et affiche les listes de protocoles contenant le protocole sélectionné.

Le groupe de protocoles est configuré selon vos paramètres. Les opérateurs peuvent sélectionner le groupe de protocoles configuré comme filtre pour un rapport d'analyse ou personnalisé.

Remarque : Les opérateurs peuvent définir des rapports uniquement si leurs paramètres d'utilisateur le permettent.

Vérification des paramètres du groupe de protocoles

Une fois que vous avez créé un groupe de protocoles et que les opérateurs l'utilisent dans des rapports, vous pouvez y apporter des modifications. Par exemple, vous pouvez renommer le groupe de protocoles pour refléter son mode d'utilisation par les opérateurs. Vous pouvez également modifier la liste des protocoles inclus dans le groupe.

Procédez comme suit :

1. Dans la page Configuration du groupe de protocoles, sélectionnez le groupe de protocoles dans la liste Groupe de protocoles.
2. (Facultatif) Modifiez le nom ou la description du groupe de protocoles :

   a. Cliquez sur Modifier.

      La page Modifier un groupe de protocoles s'ouvre.

b. Changez les valeurs des champs Nom du groupe et Description pour décrire clairement l'objectif du groupe de protocoles.

c. Cliquez sur Soumettre.

Le nom et la description sont mis à jour dans la liste de la page Configuration du groupe de protocoles et dans la page Index des groupes de protocoles.

3. (Facultatif) Révisez la liste de protocoles inclus :

a. Cliquez sur Liste.

Une table répertoriant les protocoles est ajoutée au bas de la page.

b. Sélectionnez le domaine approprié dans la liste de domaines (si les noms de protocoles personnalisés ont été définis).

Le paramètre Domaine s'affiche uniquement pour les environnements contenant plusieurs domaines.

Pour plus d'informations sur le paramètre Domaine, reportez-vous à l'étape 3 dans la rubrique Configuration du groupe de protocoles (page 104).

c. Cliquez sur Ajouter/Supprimer et modifiez le contenu du groupe de protocoles si nécessaire

Pour plus d'informations sur cette étape, reportez-vous à l'étape 4 dans la rubrique Configuration du groupe de protocoles (page 104).

d. Cliquez sur Terminé lorsque vous avez terminé de configurer le contenu du groupe de protocoles.

Le groupe de protocoles est configuré selon vos paramètres. Les opérateurs peuvent sélectionner le groupe de protocoles reconfiguré comme filtre pour un rapport d'analyse ou personnalisé.

Etiquetage de valeurs de type de service

Vous pouvez créer des étiquettes (ou descriptions) pour les valeurs de type de service afin que les opérateurs sachent à quel service ou application les différentes valeurs de type de service correspondent. Si vous n'étiquetez aucune valeur de type de service, la valeur de type de service numérique est affichée par défaut.

Remarque : Les étiquettes de type de service que vous créez concernent toutes les utilisations du type de service dans le domaine affecté, mais ne concernent pas les étiquettes de type de service d'autres domaines. Les étiquettes de type de service sont propres au domaine, dans les déploiements qui incluent plusieurs domaines.

Procédez comme suit :

1. La page Configuration du type de service s'affiche.
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu de la page Administration, sélectionnez Noms de type de service.

      La page Configuration du type de service s'ouvre et affiche des informations sur le type de service et le domaine sélectionnés.
2. (Environnement à domaines multiples) Sélectionnez le domaine qui contient les valeurs de type de service que vous voulez modifier.
3. Sélectionnez une valeur de type de service dans la liste, puis cliquez sur Modifier.

   La description peut être modifiée.
4. Saisissez une nouvelle description pour la valeur de type de service dans la zone de description et cliquez sur Enregistrer.

   La modification est enregistrée et les champs Description et Valeur pour le type de service sélectionné sont mis à jour.

Remarque : Vous pouvez également utiliser la page Configuration du type de service pour ajouter des valeurs de type de service à des groupes de types de service ou les supprimer. Sélectionnez le domaine et la valeur de type de service, puis cliquez sur le lien Ajouter/supprimer, dans la partie supérieure de la liste des groupes de types de service. La boîte de dialogue Index de groupe de types de service s'ouvre. Apportez les modifications nécessaires aux groupes configurés par les utilisateurs. Vous ne pouvez pas modifier les groupes de types de service prédéfinis.

Création et gestion des groupes de types de services

Un administrateur peut créer des groupes de types de services qui agissent comme des filtres pour les données de rapport. L'administrateur configure chaque groupe de types de service pour contenir les valeurs de types de service qui caractérisent un type particulier de trafic réseau. Les opérateurs peuvent utiliser le groupe de types de service comme filtre dans des rapports au lieu d'ajouter des filtres pour chaque valeur de types de service.

Par exemple, si les opérateurs veulent générer des rapports sur le trafic réseau pour le groupe Low Drop Assured Forwarding (acheminement assuré à faible taux d'abandon). Ce groupe est un groupe de valeurs de types de services affectées à des applications prioritaires par rapport au trafic moins critique. L'administrateur crée un groupe de types de services nommé Low drop (faible taux d'abandon), qui inclut toutes les valeurs de types de services pour AF11, AF21, AF31 et AF41. Les opérateurs peuvent créer un rapport sur le trafic des applications à l'aide du nouveau groupe Low Drop ToS (types de services de faible taux d'abandon).

Remarque : Dans un environnement qui inclut des domaines, les groupes de types de service sont disponibles dans tous les domaines, de même que les filtres pour les rapports d'analyse et les rapports personnalisés. Les étiquettes de types de service affichées pour le contenu d'un groupe de types de service sont propres à un domaine.

Création d'un groupe de types de services de shell

Créez des groupes de types de services pour permettre aux utilisateurs d'obtenir rapidement des résultats optimaux à partir des rapports d'analyse et personnalisés.

Procédez comme suit :

1. Ouvrez la page Configuration du groupe de types de services :

   a. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.

   b. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   c. Dans le menu de la page Administration, sélectionnez Groupes : Groupes de types de service.

      La page Configuration du groupe de types de service s'ouvre et affiche des informations spécifiques sur le groupe de types de services et le domaine (le cas échéant) sélectionnés.

2. Cliquez sur Ajouter.

   Les options de cette page permettent d'identifier un nouveau groupe de types de services de shell.

3. Entrez les valeurs dans les zones Nom et Description.

   Le nom et la description s'affichent aux emplacements suivants :

   - Liste des groupes de types de services sur la page Configuration du groupe de types de services
   - Index des groupes de types de services qu'un utilisateur peut afficher dans l'assistant de création de rapports pour définir un rapport d'analyse ou personnalisé

4. Cliquez sur Ajouter.

   Un nouveau groupe de types de services de shell est créé. Le nouveau nom du groupe de types de services s'affiche dans la liste de groupes de types de services sur la page Configuration du groupe de types de services.

   Vous pouvez ajouter des valeurs au groupe de types de services de shell.

Ajout de valeurs de types de services au groupe

Après la création d'un groupe de types de services de shell, l'étape suivante consiste à ajouter des valeurs au groupe.

Procédez comme suit :

1. Dans la page Configuration du groupe de types de services, sélectionnez le groupe de types de services dans la liste Groupe de types de services.

   - (Facultatif) Dans la liste de domaines, sélectionnez une combinaison client hébergé/domaine, si votre environnement inclut plusieurs domaines et étiquettes de type de service propres à chaque domaine.

   Le paramètre Domaine apparaît uniquement dans les environnements à domaines multiples.

   Sélectionnez une combinaison client hébergé/domaine pour afficher les étiquettes de types de service disponibles et spécifiques au domaine et identifier facilement les valeurs de type de service à utiliser. Le groupe de types de services ne sera pas restreint au domaine sélectionné : les groupes sont disponibles dans tous les domaines.

2. Cliquez sur Ajouter/supprimer.

   La boîte de dialogue Index des types de service s'affiche. La liste des types de services affiche les valeurs d'index de types de service et les étiquettes de types de service qui ont été définies. Dans un environnement multi-domaine, les étiquettes de types de service affichées correspondent au domaine sélectionné.

3. Sélectionnez les valeurs de types de services que vous voulez ajouter en cliquant sur les cases à cocher correspondantes.

4. Faites défiler la liste vers le bas et cliquez sur Enregistrer.

   Les valeurs sont ajoutées au groupe de types de services.

   Un opérateur peut sélectionner le groupe dans l'index de groupes de types de services lors de la définition d'un rapport d'analyse ou personnalisé.

   Remarque : Pour définir des rapports, l'opérateur doit disposer du rôle et des paramètres de groupe d'autorisations nécessaires.

Modification du contenu des groupes de types de service

Vous pouvez modifiez la liste des valeurs de type de service incluses dans un groupe de types de service afin d'apporter des corrections ou de changer le but du groupe.

Même dans un environnement multi-domaine, les groupes de types de service sont indépendants des domaines. Les valeurs de types de service incluses dans un groupe ne changent pas lorsque vous basculez vers un domaine différent.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.

   La page Administration s'ouvre.

2. Dans le menu de la page Administration, sélectionnez Groupes : Groupes de types de service.

   La page Configuration du groupe de types de service s'ouvre et affiche les informations concernant le groupe de types de service et la combinaison client hébergé/domaine (le cas échéant) sélectionnés.

3. Sélectionnez le groupe de types de service à modifier dans la liste Sélectionner un groupe de types de service.

   La page Configuration du groupe de types de service s'ouvre et affiche des informations sur le groupe de types de service et le domaine (le cas échéant) sélectionnés.

   Remarque : Vous ne pouvez pas modifier les groupes prédéfinis, comme le groupe Tous les types de service dans le domaine par défaut.

4. (Environnement à domaines multiples uniquement) Dans la liste de domaines, sélectionnez une combinaison client hébergé/domaine, si votre environnement inclut plusieurs domaines et étiquettes de type de service. Dans un environnement à domaines multiples, les étiquettes de type de service sont propres à chaque domaine.

   Le paramètre Domaine est affiché uniquement lorsque plusieurs domaines existent.

5. Cliquez sur le lien Ajouter/supprimer situé au-dessus de la liste de valeurs de type de service incluses dans le groupe.

   La boîte de dialogue Index des types de service s'affiche. La liste Type de service comprend les étiquettes de types de services qui ont été définies.

6. Cochez les cases ou désélectionnez-les pour inclure uniquement les valeurs de type de service que vous souhaitez.

7. Lorsque vous avez effectué vos modifications, cliquez sur Enregistrer. La liste des valeurs de type de service est mise à jour.

Suppression de groupes de types de service

Vous pouvez supprimer un groupe de types de service qui n'est plus utile. Une fois que vous les avez supprimés, ils ne sont plus répertoriés dans la liste des groupes de types de service.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.

   La page Administration s'ouvre.

2. Dans le menu de la page Administration, sélectionnez Groupes : Groupes de types de service.

   La page Configuration du groupe de types de service s'ouvre et affiche des informations sur le groupe de types de service et le domaine (le cas échéant) sélectionnés.

3. Sélectionnez le groupe de types de service à supprimer dans la liste Sélectionner un groupe de types de service.

   Sélectionnez un groupe de types de service configurable. Par exemple, vous ne pouvez pas modifier le groupe Tous les types de service.

   Remarque : Le paramètre Domaine, s'il existe, n'a aucun effet sur la liste des groupes de types de service disponibles. Si vous supprimez un groupe de types de service, il est supprimé pour tous les domaines.

4. Cliquez sur Supprimer.

   Un message de confirmation s'affiche.

5. Cliquez sur OK.

   Le groupe sélectionné est supprimé. La liste des valeurs de type de service est mise à jour.

Personnalisation des noms de systèmes autonomes

Les rapports d'interface contenant des données relatives au trafic des systèmes autonomes répertorient généralement ce type de trafic par nom et numéro. Les administrateurs peuvent personnaliser les noms de systèmes autonomes qui apparaîtront dans les rapports pour utiliser des noms plus courts ou descriptifs.

Par exemple, si les opérateurs consultent fréquemment des rapports sur le trafic réseau tel qu'AS 4000000. L'étiquette portant le nom du système autonome par défaut est UUNET-CANADA - Progressive Communications Services, Inc. d/b/a Acme Business (4000000). L'administrateur peut personnaliser le nom du système autonome pour afficher le nom suivant dans le rapport : Acme (4000000).

Dans un environnement multi-domaine, les noms de système autonome sont propres à chaque domaine. Dans ce type d'environnement, les noms de système autonome qui s'affichent dans les rapports sont extraits du domaine de l'interface du rapport.

Les rubriques de cette section décrivent la procédure de révision et de modification des noms de systèmes autonomes.

Pour effectuer ces tâches, configurez le flux NetFlow ou le flux compatible avec NetFlow pour la prise en charge de la génération de rapports pour des systèmes autonomes. Pour afficher des données de systèmes autonomes pertinentes dans les rapports, vous devez activer cette prise en charge, car NetFlow n'exporte pas des informations de systèmes autonomes complètes par défaut. Pour plus d'informations sur l'activation des données de systèmes autonomes, consultez l'article de la base de connaissances TEC562036, Viewing AS Numbers in Reports, sur le site de CA Support (http://ca.com/support).

Les données de systèmes autonomes affichent la valeur Système autonome 0 dans les rapports dans les cas suivants :

- Le flux n'est pas configuré pour prendre en charge la génération de rapports pour des systèmes autonomes.
- Le routage de la source des données est inconnu.
- Les données proviennent du système local.

Révision des noms de systèmes autonomes

Révisez les références des systèmes autonomes dans les rapports d'interfaces pour votre entreprise et localisez les numéros de systèmes autonomes en cours d'utilisation qui contiennent des références de systèmes autonomes longs et peu clairs.

Rapports d'interfaces qui contiennent des références de systèmes autonomes :

- Table du récapitulatif des tronçons suivants du système autonome (interface unique)
- Graphiques à secteurs, graphiques de tendance et tables de récapitulatif des N principaux systèmes autonomes

Procédez comme suit :

1. Collectez des informations concernant les noms de systèmes autonomes utilisés dans les rapports d'interface pour votre entreprise.

   La liste de tous les numéros et noms de systèmes autonomes est grande. Vous ne personnaliserez pas tous les noms de systèmes autonomes de la liste.

   Par exemple, créez la liste des noms de systèmes autonomes souvent utilisés en examinant les rapports des systèmes autonomes ou en demandant aux opérateurs quels systèmes autonomes ils suivent.

2. Affichez la page Noms des systèmes autonomes :

   a. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.

   b. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   c. Sélectionnez la page Définir une application : Noms des systèmes autonomes dans le menu de la page Administration.

      La page Noms des systèmes autonomes s'ouvre. Elle contient les informations concernant la première page de valeurs de systèmes autonomes.

3. Localisez chaque système autonome dont vous voulez personnaliser le nom :

   - Pour changer le nombre de lignes de chaque page, utilisez l'option Nombre maximum par page.
   - Pour afficher une autre page, utilisez les éléments de navigation situés au bas de la page.
   - Pour effectuer une recherche, entrez une ou plusieurs chaînes de texte dans la zone de recherche, puis cliquez sur Rechercher.

Règles de correspondance :

- Les recherches ne respectent pas la casse.
- Toutes les chaînes de recherche spécifiées doivent être trouvées dans la colonne Numéro du système autonome ou Description.
- Entourez la chaîne de recherche de guillemets droits pour limiter la recherche à l'ordre et aux mots indiqués. Par exemple, les résultats obtenus pour la chaîne de recherche *site Internet* sans guillemets peuvent inclure *site Web Internet* et *site Web*.

4. Révisez les noms de systèmes autonomes qui s'affichent dans la colonne Description.

   Vous pouvez modifier le nom de système autonome par défaut qui doit être personnalisé, dès sa localisation.

Modification de noms de systèmes autonomes

Effectuez les opérations de personnalisation nécessaires au niveau des noms des systèmes autonomes pour rendre les étiquettes des rapports d'interface plus conviviales.

Procédez comme suit :

1. (Facultatif) Révisez et corrigez le paramètre Domaine si nécessaire.

   Dans un environnement multi-domaine, les noms de système autonome sont propres à chaque domaine. Dès lors, les modifications apportées aux noms de systèmes autonomes affectent les rapports relatifs aux interfaces du domaine sélectionné.

2. Sélectionnez la ligne du numéro de système autonome que vous voulez modifier.
3. Cliquez sur Modifier.

   La boîte de dialogue Modifier la description du numéro de système autonome s'ouvre.

4. Entrez le nom personnalisé (description) dans la zone Nouveau nom.

   La valeur Ancien nom correspond au nom officiel (de base) du système autonome et vous ne pouvez pas la modifier.

5. Cliquez sur Enregistrer.

   Le nom que vous avez spécifié s'affiche dans la colonne Description pour le numéro du système autonome sélectionné. Tous les noms de systèmes autonomes personnalisés sont affichés en gras.

   Les noms de systèmes autonomes mis à jour apparaissent également dans des étiquettes et d'autres références dans les vues d'interfaces CA Network Flow Analysis suivantes :

   - Table du récapitulatif des tronçons suivants du système autonome (interface unique)
   - Graphiques à secteurs, graphiques de tendance et tables de récapitulatif des N principaux systèmes autonomes

6. Répétez ces étapes pour chaque système autonome que vous voulez personnaliser.

Remarque : Pour restaurer le nom officiel d'un système autonome, cliquez sur Réinitialiser dans la ligne appropriée, puis cliquez sur OK dans la zone de confirmation.

Chapitre 8: Opérations supplémentaires de personnalisation

Vous pouvez réaliser des opérations supplémentaires de personnalisation afin que les opérateurs puissent tirer le meilleur profit des rapports.

Une fois le produit enregistré comme source de données, vous pouvez utiliser la console Performance Center pour administrer les utilisateurs, les rôles, les profils SNMP et un grand nombre de types de groupes.

Cette section décrit la procédure à suivre pour effectuer les opérations de personnalisation suivantes dans la console NFA :

Création de filtres de temps

Créez des filtres de temps pour permettre aux utilisateurs de créer des rapports contenant des données optimisées. Par exemple, vos utilisateurs veulent plusieurs rapports qui décrivent le trafic réseau durant les heures ouvrées. Vous créez un filtre de temps qui s'applique du lundi au vendredi, de 8:00 à 17:00 heures. Vous pouvez également créer des filtres de temps pour des périodes correspondant à des opérations dans votre environnement, comme les sauvegardes automatisées.

Vous pouvez également utiliser les filtres de temps pour configurer les interruptions de la page Configuration des interruptions.

Remarque : Pour plus d'informations sur l'utilisation des filtres de temps, reportez-vous à la rubrique Création d'interruptions (page 164).

Les utilisateurs peuvent utiliser les filtres de temps personnalisés à partir de listes d'option de filtre de temps dans les emplacements suivants :

- Page Spécifier la planification de l'Assistant de création de rapports personnalisés ou de l'Assistant de création de rapports d'analyse.
- Options affichées par les opérateurs en cliquant sur le paramètre de période dans un rapport d'interface d'analyse en profondeur de types suivants : Présentation, Protocoles, Type de service, Hôtes, Conversations, Flux, Utilisation et Numéro du système autonome.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.

   La page Administration s'ouvre.

2. Sous l'étiquette Administration : Génération de rapports du menu Administration, sélectionnez Filtres de temps.

   La page Configuration du filtre de temps s'ouvre et affiche une liste des filtres de temps actuellement configurés.

3. Cliquez sur Ajouter.

   La page Configuration du filtre de temps affiche les options permettant l'ajout d'un filtre de temps.

   Configuration du filtre de temps

   Ajouter un filtre d'heure

   Nom du filtre de temps : *

   Description :

   le: lundi, mardi, mercredi, jeudi, vendredi, samedi, dimanche

   Heure de début 00 : 00 Heure de fin 00 : 00 (00:00 représente aussi bien le début que la fin du jour.)

   * Champ obligatoire

   Soumission terminée | Soumettre et ajouter | Annuler

4. Saisissez des valeurs dans les champs suivants :

   ■ Nom du filtre de temps : définissez l'identificateur de filtre de temps, qui s'affiche dans les listes suivantes.

     – Liste de la page Configuration du filtre de temps (administrateurs)

     – Les options de filtre de temps disponibles dans la page Spécifier la planification de l'Assistant de création de rapports personnalisés.

     – Les options de filtre de temps disponibles lorsqu'un utilisateur ou l'administrateur clique sur le paramètre de période dans un rapport d'interface d'analyse en profondeur des types suivants : Présentation, Protocoles, Type de service, Hôtes, Conversations, Flux, Utilisation, et Numéro du système autonome.

   ■ Description (facultatif) : ajoutez des informations pour identifier le filtre de temps qui s'affiche dans la liste des filtres de temps de la page Configuration du filtre de temps.

   ■ le : acceptez les paramètres par défaut (du lundi au vendredi) ou sélectionnez d'autres jours pour les données de rapport de collecte.

   ■ Heure de début et Heure de fin : acceptez les paramètres par défaut pour le début et la fin de la période quotidienne ou sélectionnez des paramètres personnalisés, au format 24 heures. Le paramètre par défaut de 00:00 à 00:00 inclut les données d'une période de 24 heures par jour.

     Pour, par exemple, limiter la période de génération de rapports aux heures ouvrées, sélectionnez 08:00 comme heure de début et 17:00 comme heure de fin. Pour définir un filtre pour les sauvegardes qui s'exécutent le mardi de 23 heures à 03 heures du matin le mercredi, sélectionnez Mardi, puis 23:00 et 03:00.

5. Enregistrez le filtre de temps en cliquant sur l'un des boutons suivants :
   - Soumission terminée : enregistre le filtre de temps et renvoie à la liste de filtres de temps.
   - Soumettre et ajouter : enregistre le filtre de temps et continue d'afficher les options d'ajout pour que vous puissiez configurer un autre filtre de temps.

Remarque : Pour supprimer un filtre de temps, sélectionnez-le dans la liste de filtres de temps disponibles, cliquez sur Supprimer, puis confirmez la suppression lorsque vous y êtes invité. Pour modifier un filtre de temps, sélectionnez-le dans la liste de filtres disponibles, modifiez l'une des options affichées, puis cliquez sur Soumettre.

Création de périodes de génération de rapports

Créez des périodes de génération de rapports pour optimiser les résultats des rapports. Par exemple, vos utilisateurs analysent généralement le trafic réseau sur deux semaines. Pour faciliter l'affichage des données d'interface sur cette période, créez une période de génération de rapports de deux semaines.

Les périodes de génération de rapports personnalisées sont disponibles via l'option Période lorsqu'un utilisateur ou l'administrateur clique sur le paramètre de période dans un rapport d'interface d'analyse en profondeur des types suivants : Présentation, Protocoles, Type de service, Hôtes, Conversations, Flux, Utilisation et Numéro du système autonome. Pour plus d'informations sur ces types de rapport, consultez le *Manuel de l'utilisateur CA Network Flow Analysis*.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.

   La page Administration s'ouvre.

2. Sous l'étiquette Administration : Génération de rapports du menu Administration, sélectionnez Périodes de génération de rapports.

   La page Configuration des périodes de génération de rapports s'ouvre et affiche une liste des périodes de génération de rapports actuelles, y compris les périodes de génération de rapports intégrées et personnalisées.

3. Cliquez sur Ajouter.

   Les champs et les options permettant d'ajouter une période de génération de rapports sont affichés.

4. Spécifiez les valeurs suivantes :
   - Période de génération de rapports : identificateur de la période de génération de rapports qui s'affiche dans les listes de périodes de génération de rapports disponibles suivantes :
     - Liste de la page Configuration des périodes de génération de rapports (administrateurs)
     - Les options de période sont disponibles lorsqu'un utilisateur ou l'administrateur clique sur le paramètre de période dans un rapport d'interface d'analyse en profondeur des types suivants : Présentation, Protocoles, Type de service, Hôtes, Conversations, Flux, Utilisation et Numéro du système autonome.
   - Durée : nombre et type d'unités de temps (années, mois, semaines, jours ou heures).
   - Description (facultatif) : remarques supplémentaires pour faciliter l'identification de la période de génération de rapports. La description s'affiche dans la liste de la page Configuration des périodes de génération de rapports, mais uniquement pour les administrateurs.
5. Enregistrez la période de génération de rapports en cliquant sur l'un des boutons suivants :
   - Soumission terminée : enregistre la période de génération de rapports actuelle et renvoie à la liste de périodes de génération de rapports disponibles.
   - Soumettre et ajouter : enregistre la période de génération de rapports et continue d'afficher les options d'ajout pour que vous puissiez configurer une autre période.

Remarque : Pour supprimer une période de génération de rapports, sélectionnez-la dans la liste de périodes de génération de rapports disponibles, cliquez sur Supprimer, puis confirmez la suppression lorsque vous y êtes invité. Pour modifier une période de génération de rapports, sélectionnez-la dans la liste, modifiez l'une des options affichées, puis cliquez sur Soumettre.

Configuration du mappage d'applications

Vous pouvez créer des règles de mappage d'applications afin d'identifier les types de trafic dans les rapports. Les règles permettent d'identifier des types de trafic tels qu'un type de service, un hôte, un sous-réseau ou une application NBAR2.

Vous pouvez utiliser le mappage d'applications pour grouper, différencier ou identifier plus clairement le trafic dans les rapports :

- Différenciation du trafic : vous pouvez scinder de grands blocs de trafic en remappant des sous-types de trafic avec des ports de destination distincts.

  Supposons par exemple que les rapports montrent un grand bloc de trafic FTP sur le port TCP 20. Vous voulez suivre le trafic FTP de votre serveur FTP indépendamment du trafic Internet. Pour ce faire, vous pouvez créer une règle de mappage d'applications Hôte nommée *Trafic FTP interne*. La valeur Hôte de la règle correspond à l'adresse IP du serveur FTP interne. La valeur du port est 20. Comme port de destination, spécifiez 65000, à savoir un port qui ne reçoit actuellement aucun trafic.

  Les rapports affichent maintenant le trafic du serveur FTP sur le port TCP 65000 avec l'étiquette *Trafic FTP interne*. Le trafic sur l'autre port TCP 20 est toujours étiqueté *FTP.*

- Groupement de trafic : vous pouvez générer des rapports sur une seule unité regroupant différents types de trafic en remappant ces derniers avec un seul port de destination.

  Supposons par exemple que vos systèmes de messagerie d'entreprise utilisent les protocoles IMAP et POP. Le courriel IMAP utilise le port TCP 443 et le courriel POP utilise les ports TCP 109 et 100. Vous voulez que les rapports affichent le trafic de courriel de façon groupée. Pour ce faire, vous pouvez créer des règles de mappage d'applications qui remappent chaque type de trafic de courriel avec le port 3100. Le trafic est regroupé dans les rapports et est désigné par le nom de la règle, à savoir *Courriel*. Même si vous avez créé plusieurs règles, le programme utilise le même nom pour toutes les règles qui mappent le trafic avec le port 3100.

- Identification du trafic : vous pouvez utiliser le mappage d'applications pour ré-étiqueter du trafic sans le grouper ni le scinder.

Le mappage d'applications a un impact sur les rapports suivants :

- Page Présentation de l'entreprise : rapport Principaux protocoles.
- Page Interface : tous les rapports fournissant des informations sur les protocoles.
- Page Génération de rapports personnalisés et page Analyse : index des protocoles, lequel permet de sélectionner des protocoles pour filtrer un nouveau rapport ou un rapport modifié.

Remarques :

- Le mappage d'applications n'a aucun impact sur les rapports d'examen de flux.

  Pour poursuivre l'exemple sur la différenciation des types de trafic FTP, les rapports de protocoles de session d'examen de flux montrent le trafic FTP tel qu'il était avant le mappage du sous-type de trafic FTP.

  Les rapports d'examen de flux qui affichent des données NBAR2 montrent le nom et l'ID officiels de l'application, indépendamment des éventuelles règles de mappage d'applications que vous avez configurées.

- Les rapports montrent les résultats du mappage au cours de la période d'application des règles. Si vous créez des règles aujourd'hui, les rapports sur les données de la semaine dernière ne montrent pas les effets des règles. Si vous créez, supprimez ou modifiez des règles de mappage d'applications pendant la période d'analyse, il se peut que le rapport montre un changement spectaculaire au moment de la modification des règles.

Vous pouvez effectuer les opérations de mappage d'applications suivantes :

- Utiliser les fonctions d'administration de la console NFA pour configurer ou modifier des règles de mappage d'applications afin de regrouper ou de scinder des données :
  - Créer une règle de mappage d'applications Tout (type de service) (page 126)
  - Créer une règle de mappage d'applications Hôte (page 127)
  - Créer une règle de mappage d'applications Sous-réseau (page 129)
  - Créer une règle de mappage d'applications NBAR2 (page 131)
  - Modifier des règles de mappage d'applications (page 133)
- Configurer des paramètres globaux pour la prise en charge des règles de mappage dans les rapports (page 124)
- Comprendre le fonctionnement des priorités pour les règles de mappage d'applications (page 124)
- Effectuer des opérations d'importation par lots à l'aide d'un fichier .csv :
  - Importer les règles de mappage d'applications NBAR2 par défaut (page 134)
  - Importer des règles de mappage d'applications personnalisées (page 136)
  - Importer des mises à jour de règle de mappage d'applications (page 139)
  - Passer en revue les erreurs d'importation de règles (page 142)

Mappage d'applications : priorités

Si un flux entrant réunit les critères spécifiés dans une règle de mappage d'applications, il est mappé avec le port de destination défini dans la règle. En cas de conflit entre des règles, les priorités suivantes s'appliquent. Une règle à la priorité lorsque ses critères sont supérieurs aux critères d'une autre règle.

- *Priorité 1 :* règle Hôte avec paramètres Hôte, Protocole, Port et Type de service spécifiés
- *Priorité 2 :* règle Hôte avec paramètres Hôte, Protocole et Port spécifiés, mais avec paramètre Type de service défini sur Tout
- *Priorité 3 :* règle Tout (Type de service) avec paramètre Type de service spécifié
- *Priorité 4 :* règle Hôte avec paramètre Hôte spécifié, mais avec paramètres Protocole et Type de service définis sur Tout
- *Priorité 5 :* règle Sous-réseau
- *Priorité 6 :* règle NBAR2

Configuration des paramètres globaux pour le mappage d'applications

Vérifiez les paramètres globaux qui affectent les mappages d'applications. Effectuez les modifications nécessaires pour personnaliser le comportement des mappages d'applications. Les paramètres globaux qui affectent le mappage d'applications incluent les options suivantes :

- *Port de redirection TCP :* port cible pour le trafic TCP redirigé. Si une règle de mappage d'applications envoie le trafic TCP vers un port qui reçoit déjà du trafic (non mappé), ce trafic natif est redirigé vers le port de redirection TCP.
- *Masque du type de service :* indique si tous les bits de type de service sont utilisés pour les valeurs de type de service.
- *Port de redirection UDP :* port cible pour le trafic UDP redirigé. Le port de redirection UDP reçoit le trafic UDP natif redirigé, de la même manière que le port de redirection TCP reçoit le trafic TCP natif redirigé.
- *Conserver le protocole de mappage ToS :* détermine si les valeurs de protocole sont incluses dans les rapports en plus des valeurs de type de service.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche.

2. Cliquez sur Paramètres supplémentaires.

   La page Paramètres de l'application s'affiche.

3. Vérifiez et corrigez les paramètres globaux qui affectent les mappages d'applications :

   - *Port de redirection TCP :* port cible pour le trafic TCP natif redirigé. Il est utilisé si une règle de mappage d'applications envoie le trafic TCP vers un port qui reçoit déjà un trafic natif (non mappé).

     Supposons par exemple que vous créez une règle de mappage d'applications qui a le port 655 comme le port de destination. Vous définissez le port de redirection TCP sur la valeur 630. Si le port 655 reçoit de trafic natif (non mappé), ce dernier est redirigé vers le port 630.

     Remarque : Le port de redirection est utilisé pour éviter toute fusion du trafic mappé avec d'autres types de trafic. Si les règles de mappage d'applications sont configurées avec des ports de destination inutilisés, le port de redirection n'est pas utilisé. Le cas échéant, les rapports ne montrent aucun trafic sur le port de redirection. Si vos rapports affichent le trafic sur le port de redirection, vous pouvez spécifier un nouveau port de destination pour le trafic mappé. Examinez le trafic sur le port de redirection afin de déterminer quelles sont les règles impliquées.

   - *Masque du type de service :* limite les valeurs de type de service de 8 bits incluses dans les rapports pour les flux. La valeur par défaut pour ce paramètre est 255, ce qui correspond à l'activation de tous les bits de type de service.

   - *Port de redirection UDP :* port cible qui redirige le trafic UDP natif, de la même manière que le port de redirection TCP redirige le trafic TCP natif.

   - *Conserver le protocole de mappage ToS :* détermine si les valeurs de protocole sont incluses dans les rapports en plus des valeurs de type de service. O (Oui) conserve les protocoles utilisés et les données de types de service sont incluses dans les rapports séparément. N (Non) affiche les valeurs de type de service pour le trafic, mais pas les protocoles impliqués. Le paramètre par défaut est O.

4. Cliquez sur Enregistrer.

   Vos modifications sont enregistrées. La page Paramètres de l'application reste affichée.

Création d'une règle de mappage d'applications Tout (type de service)

Vous pouvez créer une règle de mappage d'applications Tout pour regrouper, différencier ou identifier plus clairement du trafic sur la base de sa valeur Type de service.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
    a. Dans le menu de console NFA, sélectionnez Administration.

        La page Administration s'ouvre.

    b. Dans le menu Administration, sélectionnez Définitions d'application.

    La page Définitions d'application s'affiche.
2. Vérifiez que Mappage d'applications est la valeur sélectionnée pour Règles.
3. Cliquez sur Ajouter une règle.

    La boîte de dialogue Ajouter un mappage d'applications s'ouvre.
4. Dans la liste de types de règle de la partie supérieure de la boîte de dialogue, sélectionnez Tout.

    La boîte de dialogue Ajouter un mappage d'applications passe en mode de règle Tout (type de service).
5. Définissez la valeur du paramètre suivant :
    - Type de service : type de service à utiliser comme filtre pour les données collectées.

        Lors de l'ouverture de la boîte de dialogue, la valeur par défaut est Tout. Si vous ne modifiez pas cette valeur, le trafic correspondant à toutes les valeurs de type de service est mappé avec le port de destination.
    - Port de destination : port cible qui collecte les données mappées.

        Si vous spécifiez un port de destination qui est déjà utilisé par d'autres règles, le trafic auquel s'appliquent les règles en question sera groupé.
    - (Facultatif) Cliquez sur Vérifier afin d'exécuter un contrôle général pour déterminer si le port spécifié reçoit déjà des données. Le contrôle échoue si le port reçoit des données natives, autrement dit, des données qui ne sont pas mappées par des règles de mappage d'applications. Si le port de destination spécifié reçoit des données natives, ces dernières sont redirigées vers le port de redirection (page 124).

- Nom : identificateur de la règle tel qu'elle est répertoriée dans la page Définitions d'application.

  Dans certains rapports, le nom de la règle est également l'étiquette du trafic mappé. Si d'autres règles mappent du trafic avec le même port de destination que celui spécifié pour cette règle, indiquez le nom à utiliser pour le trafic groupé.

- Description : (facultatif) texte descriptif supplémentaire permettant d'identifier le type de règle et son utilisation, qui est affiché uniquement dans la page Définitions d'applications.

6. Cliquez sur Enregistrer.

   La boîte de dialogue se ferme. La nouvelle règle est ajoutée à la liste des règles de mappage d'applications. Si une autre règle mappe du trafic avec le même port et que vous spécifiez un nouveau nom de règle, les autres noms de règle sont mis à jour.

7. (Facultatif) Exécutez des rapports pour vérifier que le trafic sur le port cible de destination spécifié la règle.

8. (Facultatif) Examinez les effets des règles de mappage d'applications créées ou modifiées sur les rapports, puis renommez éventuellement la règle afin d'identifier plus clairement le trafic mappé dans les rapports.

Création d'une règle de mappage d'applications d'hôte

Vous pouvez créer une règle de mappage d'applications Hôte pour regrouper, différencier ou identifier plus clairement du trafic sur la base de son h^te source. Par exemple, une règle d'application Hôte peut permettre d'inclure dans les rapports le trafic total d'un serveur spécifique ou d'une application sur le serveur.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Définitions d'application.

   La page Définitions d'application s'affiche.

2. Vérifiez que Mappage d'applications est la valeur sélectionnée pour Règles.

3. Cliquez sur Ajouter une règle.

   La boîte de dialogue Ajouter un mappage d'applications s'ouvre.

4. Sélectionnez Hôte dans la liste de types de règle dans la partie supérieure de la boîte de dialogue.

   La boîte de dialogue Ajouter un mappage d'applications passe en mode de règle Hôte.

5. Saisissez des valeurs pour les paramètres suivants :

   - Hôte : adresse IP du serveur pour lequel vous mappez le trafic réseau.
   - Type de service : type de service à utiliser comme filtre pour les données collectées. Pour que toutes les valeurs de type de service correspondent, acceptez la valeur par défaut Tout ou laissez la zone Type de service vide.
   - Protocole : protocole des données affecté par la règle (TCP ou UDP).
   - Port : port à utiliser pour la collecte de données. Pour que toutes les valeurs de port correspondent, acceptez la valeur par défaut Tout ou laissez la zone Port vide.
   - Port de destination : port cible qui collecte les données mappées.

     Si vous spécifiez un port de destination qui est déjà utilisé par d'autres règles, le trafic auquel s'appliquent les règles en question sera groupé.
   - (Facultatif) Cliquez sur Vérifier afin d'exécuter un contrôle général pour déterminer si le port spécifié reçoit déjà des données. Le contrôle échoue si le port reçoit des données natives, autrement dit, des données qui ne sont pas mappées par des règles de mappage d'applications. Si le port de destination spécifié reçoit des données natives, ces dernières sont redirigées vers le port de redirection (page 124).
   - Nom : identificateur de la règle tel qu'elle est répertoriée dans la page Définitions d'application.

     Dans certains rapports, le nom de la règle est également l'étiquette du trafic mappé. Si d'autres règles mappent du trafic avec le même port de destination que celui spécifié pour cette règle, indiquez le nom à utiliser pour le trafic groupé.
   - Description : (facultatif) texte descriptif supplémentaire permettant d'identifier le type de règle et son utilisation, qui est affiché uniquement dans la page Définitions d'applications.

6. Cliquez sur Enregistrer.

   La boîte de dialogue se ferme. La nouvelle règle est ajoutée à la liste des règles de mappage d'applications. Si une autre règle mappe du trafic avec le même port et que vous spécifiez un nouveau nom de règle, les autres noms de règle sont mis à jour.

7. (Facultatif) Exécutez des rapports pour vérifier que le trafic sur le port cible de destination spécifié la règle.
8. (Facultatif) Examinez les effets des règles de mappage d'applications créées ou modifiées sur les rapports, puis renommez éventuellement la règle afin d'identifier plus clairement le trafic mappé dans les rapports.

Création d'une règle de mappage d'applications de sous-réseau

Vous pouvez créer une règle de mappage d'applications Sous-Réseau pour regrouper, différencier ou identifier plus clairement le trafic provenant d'un sous-réseau ou masque particulier. Par exemple, une règle Sous-Réseau peut permettre d'afficher le trafic total d'une application dans les rapports.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche.
2. Vérifiez que Mappage d'applications est la valeur sélectionnée pour Règles.
3. Cliquez sur Ajouter une règle.

   La boîte de dialogue Ajouter un mappage d'applications s'ouvre.
4. Vérifiez que Sous-Réseau est sélectionné comme type de règle dans la partie supérieure de la boîte de dialogue. Cette option est sélectionnée par défaut.

   La boîte de dialogue Ajouter un mappage d'applications affiche les options pour une règle de mappage d'applications de sous-réseau.
5. Saisissez des valeurs pour les paramètres suivants :
   - Sous-réseau : adresse IP de la source de données, au format décimal séparé par des points. Pour spécifier un sous-réseau qui correspond à toutes les adresses, utilisez 0.0.0.0/0 comme sous-réseau et comme masque.
   - Masque : masque à appliquer au sous-réseau.
   - Protocole : protocole des données affecté par la règle (TCP ou UDP).
   - Port de début : port de début de la plage de ports pour la collecte de données, au format décimal de base 10. Le port de début est inclus dans la plage de ports. La valeur de port maximum permise est 65535.
   - Port de fin : dernier port de la plage à utiliser pour la collecte de données. Le port de fin est inclus dans la plage de ports.

- Port de destination : port cible qui collecte les données mappées.

  Si vous spécifiez un port de destination qui est déjà utilisé par d'autres règles, le trafic auquel s'appliquent les règles en question sera groupé.

- (Facultatif) Cliquez sur Vérifier afin d'exécuter un contrôle général pour déterminer si le port spécifié reçoit déjà des données. Le contrôle échoue si le port reçoit des données natives, autrement dit, des données qui ne sont pas mappées par des règles de mappage d'applications. Si le port de destination spécifié reçoit des données natives, ces dernières sont redirigées vers le port de redirection (page 124).

- Nom : identificateur de la règle tel qu'elle est répertoriée dans la page Définitions d'application.

  Dans certains rapports, le nom de la règle est également l'étiquette du trafic mappé. Si d'autres règles mappent du trafic avec le même port de destination que celui spécifié pour cette règle, indiquez le nom à utiliser pour le trafic groupé.

- Description : (facultatif) texte descriptif supplémentaire permettant d'identifier le type de règle et son utilisation, qui est affiché uniquement dans la page Définitions d'applications.

6. Cliquez sur Enregistrer.

   La boîte de dialogue se ferme. La nouvelle règle est ajoutée à la liste des règles de mappage d'applications. Si une autre règle mappe du trafic avec le même port et que vous spécifiez un nouveau nom de règle, les autres noms de règle sont mis à jour.

7. (Facultatif) Exécutez des rapports pour vérifier que le trafic sur le port cible de destination spécifié la règle.

8. (Facultatif) Examinez les effets des règles de mappage d'applications créées ou modifiées sur les rapports, puis renommez éventuellement la règle afin d'identifier plus clairement le trafic mappé dans les rapports.

Création d'une règle de mappage d'applications NBAR2

Vous pouvez créer des règles de mappage d'applications NBAR2 (Next Generation Network-Based Application Recognition) pour identifier le trafic des applications NBAR2 dans les rapports (page 122). Les règles NBAR2 permettent d'identifier le trafic d'applications distinctes, de grouper le trafic de plusieurs applications ou de dissocier le trafic NBAR2 d'autres trafics.

Si plusieurs règles mappent du trafic avec le même port de destination, le programme donne le même nom à ces règles (dernier nom spécifié). Le nom de la règle sert d'étiquette pour identifier le trafic NBAR2 dans les rapports.

Cette rubrique explique comment créer des règles de mappage d'applications NBAR2 dans la page Définitions d'applications. Vous également importer des lots de règles de mappage d'applications NBAR2 à l'aide de la ligne de commande. Pour plus d'informations sur les options d'importation via la ligne de commande, reportez-vous aux rubriques commençant par Importation de règles de mappage d'applications (page 134).

Remarques :

- Pour pouvoir afficher des données NBAR2 dans des rapports, vos routeurs doivent être configurés pour renvoyer des flux IPFIX incluant les champs NBAR2 appropriés.
- Le mappage d'applications prend en charge les règles pour les applications identifiées par le moteur NBAR2 Cisco standard (moteur NBAR2 13). En revanche, les règles pour les applications identifiées par des moteurs NBAR2 personnalisés ne sont pas prises en charge.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Définitions d'application.

   La page Définitions d'application s'affiche.
2. Vérifiez que Mappage d'applications est la valeur sélectionnée pour Règles.
3. Cliquez sur Ajouter une règle.

   La boîte de dialogue Ajouter un mappage d'applications s'ouvre.
4. Sélectionnez NBAR2 dans la liste des types de règle.

   La boîte de dialogue passe en mode de règle NBAR2.

5. Saisissez des valeurs pour les paramètres suivants :

   - ID de l'application NBAR2 : ID d'application défini par le moteur NBAR2 standard.

     Veillez à indiquer correctement l'ID d'application, faute de quoi la règle ne fonctionnera pas comme prévu. Les ID d'application sont inclus dans le fichier nbar2.csv situé dans le dossier <chemin_installation>/reporter/racmd.

   - Port de destination : port cible qui collecte les données mappées.

     Si vous spécifiez un port de destination qui est déjà utilisé par d'autres règles, le trafic auquel s'appliquent les règles en question sera groupé.

     (Facultatif) Cliquez sur Vérifier afin d'exécuter un contrôle général pour déterminer si le port spécifié reçoit déjà des données. Le contrôle échoue si le port reçoit des données natives, autrement dit, des données qui ne sont pas mappées par des règles de mappage d'applications. Si le port de destination spécifié reçoit des données natives, ces dernières sont redirigées vers le port de redirection (page 124).

   - Nom : identificateur de la règle tel qu'elle est répertoriée dans la page Définitions d'application.

     Dans certains rapports, le nom de la règle est également l'étiquette du trafic mappé. Si d'autres règles mappent du trafic avec le même port de destination que celui spécifié pour cette règle, indiquez le nom à utiliser pour le trafic groupé.

   - Description : (facultatif) texte descriptif supplémentaire permettant d'identifier le type de règle et son utilisation, qui est affiché uniquement dans la page Définitions d'applications.

   Remarque : La valeur du champ ID du moteur NBAR2 est prédéfinie et ne peut pas être modifiée. Cette valeur est définie sur 13, à savoir le moteur NBAR2 standard.

6. Cliquez sur Enregistrer.

   La boîte de dialogue se ferme. La nouvelle règle est ajoutée à la liste des règles de mappage d'applications. Si une autre règle mappe du trafic avec le même port et que vous spécifiez un nouveau nom de règle, les autres noms de règle sont mis à jour.

7. (Facultatif) Exécutez des rapports pour vérifier que le trafic sur le port cible de destination spécifié la règle.

8. (Facultatif) Examinez les effets des règles de mappage d'applications créées ou modifiées sur les rapports, puis renommez éventuellement la règle afin d'identifier plus clairement le trafic mappé dans les rapports.

Modification de règles de mappage d'applications

Modifiez une règle de mappage d'applications lorsque voulez-vous changer le port ou la plage de ports source, le port de destination, le protocole, l'hôte, le type de service, le sous-réseau, le masque, le nom de règle, la description de règle ou le type de règle.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche.
2. Cochez la case en regard de la règle.
3. Cliquez sur Modifier.

   La boîte de dialogue Modifier un mappage d'applications s'ouvre.
4. Apportez les modifications nécessaires.
5. Cliquez sur Enregistrer.

   Si les modifications sont appliquées correctement, la boîte de dialogue se ferme. La liste des règles est mise à jour pour prendre en compte vos modifications. Si plusieurs règles mappent du trafic vers le même port de destination et que vous changez le nom d'une des règles, les autres noms sont mis à jour en conséquence. Ce nom est utilisé comme étiquette pour le trafic regroupé dans les rapports.

Remarque : Vous pouvez supprimer une ou plusieurs règles en cochant les cases correspondantes et en cliquant sur Supprimer.

Importation de règles de mappage d'applications

Vous pouvez créer ou mettre à jour des règles de mappage d'applications en important un fichier .csv formaté pour le type de règle. Vous pouvez effectuer plusieurs types d'importations de règles de mappage d'applications :

- Importation de règles de mappage d'applications personnalisées (page 136)
- Importation des règles de mappage d'applications NBAR2 par défaut (page 134)
- Importation de mises à jour de règles de mappage d'applications (page 139)

Les effets et caractéristiques suivants sont associés à l'importation de règles :

- Après l'importation, les règles créées ou mises à jour figurent dans la liste de la page Définitions d'applications.
- Dans les rapports, le trafic mappé est identifié au moyen d'étiquettes correspondant aux nouveaux noms de règles, comme expliqué dans la rubrique Configuration du mappage d'applications (page 122).
- Effectuez ce type d'opération d'importation localement. L'importation ne peut pas être réalisée à distance.
- Vous pouvez travailler sur les règles de mappage d'applications dans une feuille de calcul Microsoft Excel et ensuite les exporter au format CSV.
- Si vous importez l'ensemble de règles NBAR2 par défaut, chaque application NBAR2 est mappée par défaut vers un port distinct. La plage de ports par défaut inclut les ports 65001 et supérieurs.

Remarque : Pour plus d'informations sur les échecs d'importation et messages d'erreur potentiels, reportez-vous à la rubrique Erreurs d'importation de règles de mappage (page 142).

Importation des règles de mappage d'applications NBAR2 par défaut

Vous pouvez ajouter un ensemble complet de règles de mappage d'applications NBAR2 par défaut dans le cadre d'une opération d'importation par lot. Cette tâche s'effectue dans la ligne de commande au moyen du fichier nbar2.csv fourni avec le produit.

Remarque : Les règles de mappage d'applications NBAR2 importées correspondent à l'ensemble de définitions d'applications NBAR2 existantes au moment du lancement du produit.

Procédez comme suit :

1. Connectez-vous au serveur de la console NFA en tant qu'utilisateur membre du groupe Administrateurs.
2. Ouvrez une invite de commande.

3. Accédez au répertoire contenant le fichier nbar2.csv et entrez la commande suivante :
   ```
   cd <chemin_installation>\reporter\racmd
   ```
   où :

   la variable <chemin_installation> correspond au chemin d'installation du produit. Le chemin par défaut est C:\CA\NFA.

   racmd correspond au répertoire qui contient le fichier nbar2.csv. Le fichier est écrit dans ce répertoire lorsque vous installez le produit.

4. Entrez la commande suivante :
   ```
   racmd -import nbar2.csv
   ```
   où :

   nbar2.csv est le nom du fichier de règles de mappage d'applications que vous souhaitez importer. Cette chaîne de commande est définie en partant du principe que les fichiers de commande racmd et .csv sont à leur emplacement par défaut. Si vous avez déplacé le fichier .csv, spécifiez le chemin complet (le chemin et le nom de fichier).

   En cas d'erreurs pendant l'importation, des messages d'erreur s'affichent (page 142). Si aucun message n'est renvoyé, cela signifie que l'importation s'est déroulée sans problèmes.

5. (Facultatif) Vérifiez que les règles figurent dans la liste de la page Définitions d'applications :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche. Les nouvelles règles figurent dans la liste de la page Définitions d'applications.

6. (Facultatif) Vérifiez que le trafic d'applications NBAR2 mappé est étiqueté correctement aux emplacements suivants :

   - Page Présentation de l'entreprise : rapport Principaux protocoles
   - Page Interface : tous les rapports fournissant des informations sur les protocoles.
   - Page Génération de rapports personnalisés et page Analyse : Index des protocoles, qui permet de sélectionner des protocoles pour filtrer un nouveau rapport ou un rapport modifié.

7. (Facultatif) Vous pouvez sélectionner des applications et regrouper les données relatives à leur trafic dans les rapports.

    a. Identifiez un ensemble d'applications dont vous souhaitez regrouper les données de trafic.

    b. Modifiez les règles d'application correspondantes pour envoyer les données vers un seul port de destination.

       Par défaut, chaque application NBAR2 est mappée avec un port distinct. Les ports par défaut sont supérieurs à 65000.

    c. Utilisez un nom approprié pour les règles, autrement dit, choisissez un nom qui reflète le type d'applications incluses.

       Dans les rapports, ce nom est utilisé pour identifier le trafic groupé.

       Si vous modifiez le nom d'une règle, toutes les règles qui utilisent ce port de destination sont renommées pour correspondre à la nouvelle définition. Le nom de la règle et l'étiquette sont définis lorsque vous modifiez le dernier nom de règle.

Importation de règles de mappage d'applications personnalisées

Vous pouvez créer des règles de mappage d'applications d'un type unique en important un fichier .csv correctement formaté. Des fichiers .csv d'exemple sont fournis. Ceux-ci montrent les champs à inclure obligatoirement dans le fichier d'importation pour chaque type de règle.

Procédez comme suit :

1. Connectez-vous au serveur de la console NFA en tant qu'utilisateur membre du groupe Administrateurs.

2. Ouvrez une invite de commande.

3. Ouvrez l'exemple de fichier d'importation pour votre type de règle :

    - Règle Tout (type de service) : tos.csv
    - Règle Hôte avec protocole spécifié : server-protocol.csv
    - Règle Hôte sans protocole spécifié : server.csv
    - Règle Sous-réseau : subnet.csv
    - Règle NBAR2 : nbar2.csv

4. Suivez le format dans le fichier d'exemple pour votre type de règle :

    - La première ligne dans le fichier est la ligne des noms de colonnes, qui identifie les champs. Laissez-la exactement comme elle est dans le fichier d'exemple. Ne modifiez pas l'orthographe ni l'ordre des noms de colonnes dans la ligne.
    - En dessous de la première ligne, ajoutez une ligne pour chaque règle à importer.

- Spécifiez les valeurs pour chaque champ obligatoire.

  Séparez les valeurs de champ par des virgules. N'insérez pas de virgules dans les chaînes de valeur. Une virgule indique à l'utilitaire d'importation qu'il doit passer au champ suivant.

  Hormis le champ desc (description), tous les autres sont obligatoires. Pour laisser le champ desc vide, entrez uniquement une virgule (sans espace).

- Les colonnes du fichier d'importation correspondent aux colonnes suivantes de la page Définitions d'applications :

  - name = Nom : nom de la règle
  - desc = Description (facultative)
  - protocolName = Protocole
    Pour spécifier tous les protocoles, entrez la valeur -1.
  - tos = Type de service
    Pour spécifier tous les types de service, entrez la valeur -1.
  - ip = IP/Sous-réseau : adresse IP de l'hôte
  - mask = IP/Sous-réseau : ajout du réseau à l'adresse IP de l'hôte
  - newPort = Port de destination
  - beginPort = Port de début : premier port d'une plage de ports ou numéro de port pour une règle serveur-protocole.
  - endPort = Port de fin : dernier port d'une plage de ports.
  - applicationID = ID de l'application NBAR2

  Certains champs s'appliquent uniquement à des types de règle spécifiques, comme le montre le tableau ci-dessous.

5. Accédez au répertoire qui contient le fichier .csv. La commande suivante indique l'emplacement par défaut :
   ```
   cd <chemin_installation>\reporter\racmd
   ```
   où :

   la variable <chemin_installation> correspond au chemin d'installation du produit. Par défaut, le chemin d'installation du produit est C:\CA\NFA.

   racmd correspond au répertoire qui contient le fichier d'importation .csv. Le fichier est écrit dans ce répertoire lorsque vous installez le produit.

6. Lancez l'importation en entrant la commande suivante :
   `racmd -import nbar2.csv`

   où :

   nbar2.csv est le nom du fichier de règles de mappage d'applications que vous souhaitez importer. Cette chaîne de commande est définie en partant du principe que les fichiers de commande racmd et .csv sont à leur emplacement par défaut. Si vous avez déplacé le fichier .csv, spécifiez le chemin complet (le chemin et le nom de fichier).

   En cas d'erreurs pendant l'importation, des messages d'erreur s'affichent (page 142). Si aucun message n'est renvoyé, cela signifie que l'importation s'est déroulée sans problèmes.

7. (Facultatif) Vérifiez que les règles figurent dans la liste de la page Définitions d'applications :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche.

8. (Facultatif) Vérifiez que le trafic d'applications est étiqueté correctement aux emplacements suivants :

   - Page Présentation de l'entreprise : rapport Principaux protocoles
   - Page Interface : tous les rapports fournissant des informations sur les protocoles.
   - Page Génération de rapports personnalisés et page Analyse : Index des protocoles, qui permet de sélectionner des protocoles pour filtrer un nouveau rapport ou un rapport modifié.

9. (Facultatif) Vous pouvez regrouper ou dissocier le trafic des applications sélectionnées, comme expliqué dans la rubrique Configuration du mappage d'applications (page 122).

Le tableau suivant répertorie les champs qui s'appliquent à chaque type de règle. Placez les champs dans le même ordre que dans l'exemple de fichier d'importation, et non dans l'ordre du tableau.

Type de règle	name	desc	protocolName	tos	ip	mask	newPort	beginPort	endPort	applicationID
Tout - type de service	Y	Y		Y			Y			
Hôte - serveur	Y	Y			Y		Y			
Hôte - serveur-protocole	Y	Y	Y	Y	Y		Y	Y		

Type de règle	name	desc	protocolName	tos	ip	mask	newPort	beginPort	endPort	applicationID
NBAR2 - nbar2	Y	Y					Y			Y
Sous-réseau - sous-réseau	Y	Y	Y		Y	Y	Y	Y	Y	

Importation de mises à jour de règles de mappage d'applications

Vous pouvez créer des règles de mappage d'applications d'un type unique en important un fichier .csv correctement formaté. Des fichiers .csv d'exemple sont fournis. Ceux-ci montrent les champs à inclure dans chaque type de fichier d'importation.

Procédez comme suit :

1. Connectez-vous au serveur de la console NFA en tant qu'utilisateur membre du groupe Administrateurs.
2. Identifiez l'ID des règles existantes que vous souhaitez mettre à jour.
   a. Ouvrez une invite de commande et placez-vous dans le répertoire qui contient le fichier .csv. La commande suivante indique l'emplacement par défaut :
   ```
   cd <chemin_installation>\reporter\racmd
   ```
   où :

   la variable <chemin_installation> correspond au chemin d'installation du produit. Par défaut, le chemin d'installation du produit est C:\CA\NFA.

   racmd correspond au répertoire qui contient le fichier d'importation .csv. Le fichier est écrit dans ce répertoire lorsque vous installez le produit.

   b. Exportez les définitions de règles en entrant la commande suivante :
   ```
   racmd -export csv
   ```
   Le fichier d'exportation est nommé getapplicationmapping_<horodatage>.csv. Le fichier se trouve dans le dossier en cours.

   La commande renvoie le message de statut suivant : Creating csv file (Création du fichier .csv en cours). Une fois l'opération terminée, l'invite de commande réapparaît.

   Remarque : Les ID de règles sont propres au système autonome ou de console NFA en cours.
3. Ouvrez le fichier d'exportation dans une feuille de calcul ou un éditeur de texte.

   Le fichier d'exportation contient une ligne pour chaque règle de mappage d'applications actuelle, qui commence par l'ID de règle. La ligne inclut également des informations complémentaires que vous pouvez ignorer.
4. Recherchez et notez l'ID de chaque règle que vous voulez modifier.

5. Préparez le fichier d'importation :

   a. Ouvrez une copie de l'exemple de fichier d'importation pour votre type de règle :

      - Règle Tout (type de service) : tos.csv
      - Règle Hôte avec protocole spécifié : server-protocol.csv
      - Règle Hôte sans protocole spécifié : server.csv
      - Règle Sous-réseau : subnet.csv
      - Règle NBAR2 : nbar2.csv

   b. Ajoutez la colonne appID et les valeurs de règle, comme indiqué dans les exemples suivants :

      Exemple : Deux premières lignes d'un fichier d'importation pour ajouter des règles NBAR2

      ```
      name,desc,newPort,applicationid
      youtube,Youtube video streaming,65035,82
      ```

      où :

      name = nom de la règle
      desc = description de la règle
      newPort = port de destination
      applicationID = ID de l'application NBAR2

      Exemple : Deux premières lignes d'un fichier d'importation pour modifier des règles NBAR2

      ```
      appID,name,desc,newPort,applicationid
      35,YouTube,Youtube video streaming,65035,82
      ```

      où :

      appID = ID de règle

      Si vous mettez à jour des règles de mappage d'applications NBAR2, ne changez pas la valeur du paramètre ID de l'application NBAR2. Si vous modifiez cette valeur, la règle ne fonctionnera pas comme prévu.

   c. Au lieu d'ajouter la colonne appID et les valeurs, vous pouvez aussi suivre les instructions relatives à l'importation de règles de mappage figurant à l'étape 4 de la rubrique Importation de règles de mappage d'applications personnalisées (page 136).

   d. Enregistrez le fichier d'importation.

      Il est recommandé d'enregistrer le fichier d'importation dans le répertoire qui contient la commande d'importation : <chemin_installation>\reporter\racmd.

6. Accédez au répertoire qui contient le fichier .csv :
   ```
   cd <chemin_installation>\reporter\racmd
   ```
   où :

   la variable <chemin_installation> correspond au chemin d'installation du produit. Par défaut, le chemin d'installation du produit est C:\CA\NFA.

   racmd correspond au répertoire qui contient le fichier d'importation .csv. Le fichier est écrit dans ce répertoire lorsque vous installez le produit.

7. Entrez la commande suivante :
   ```
   racmd -import nbar2_updated.csv
   ```
   où :

   nbar2_updated.csv est le nom du fichier de mises à jour que vous venez de créer. Si vous avez déplacé le fichier .csv, spécifiez le chemin complet (le chemin et le nom de fichier).

   En cas d'erreurs pendant l'importation, des messages d'erreur s'affichent (page 142). Si aucun message n'est renvoyé, cela signifie que l'importation s'est déroulée sans problèmes.

8. (Facultatif) Vérifiez que les règles mises à jour figurent bien dans la liste de la page Définitions d'applications :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche.

9. (Facultatif) Vérifiez que le trafic d'applications est étiqueté correctement aux emplacements suivants :

   - Page Présentation de l'entreprise : rapport Principaux protocoles
   - Page Interface : tous les rapports fournissant des informations sur les protocoles.
   - Page Génération de rapports personnalisés et page Analyse : Index des protocoles, qui permet de sélectionner des protocoles pour filtrer un nouveau rapport ou un rapport modifié.

Messages d'erreur lors de l'importation de règles

Cette rubrique décrit quelques-uns des messages d'erreur qui peuvent apparaître. Lorsqu'une importation est terminée, la commande renvoie des messages d'erreur pour tout échec d'importation, puis répertorie les champs pour les règles ayant échoué.

Si le fichier d'importation de règle contient des erreurs de définition de colonne, l'opération d'importation échoue. Si le fichier contient des erreurs dans des définitions de règle, l'opération d'importation ignore chaque règle défectueuse et poursuit avec la règle suivante.

Remarques concernant le champ Description :

- Tous les champs de règle doivent contenir des valeurs, sauf le champ Description (desc) facultatif. Toutefois, la ligne de règle doit inclure la virgule pour le champ Description.
- Si les valeurs du champ Description contiennent des virgules internes, l'importation de la règle échoue. L'utilitaire d'importation ne prend pas en charge des virgules dans les valeurs Description.

Une colonne nommée XXX appartient déjà à cette table de données

Le fichier d'importation contient un double de la colonne nommée dans le message d'erreur. Le nom de la colonne est affiché à la place de XXX.

Solution : supprimez la colonne dupliquée. Respectez le format dans le fichier d'exemple approprié, comme le décrit la section Importation de règles de mappage d'applications personnalisées (page 136).

Mappage d'application non valide

Un des problèmes suivants s'est produit lors de la mise à jour des règles existantes :

- Le fichier d'importation ne spécifie pas correctement l'ID d'application de la règle d'origine.
- L'ID d'application spécifié correspond à une règle qui a été supprimée.

Solution : vérifiez que l'ID d'application est entré correctement et que sa règle existe encore. Vous pouvez exporter les règles actuelles dans un fichier CSV comme le décrit la section Importation de mises à jour de règles de mappage d'applications (page 139). Le fichier d'exportation inclut les ID d'application pour toutes les règles actuelles.

L'objet Mappage d'applications n'est pas valide : un enregistrement existant est déjà en cours d'utilisation

Les deux conditions suivantes sont remplies :

- Vous utilisez le format de fichier pour importer une nouvelle règle.
- Une des définitions de règle dans le fichier d'importation a les mêmes valeurs de champ qu'une règle existante.

Solution : si cette erreur se produit rarement, vous pouvez modifier les règles séparément dans la page Définitions d'applications. Pour mettre à jour un groupe de règles existantes à l'aide de la commande racmd, utilisez le format de fichier d'importation décrit à la section Importation de mises à jour de règles de mappage d'applications (page 139).

L'objet Mappage d'applications n'est pas valide : un protocole non valide a été entré

Le fichier d'importation peut contenir un nom de colonne mal orthographié ou inclure une colonne non valide. Cette erreur peut également se produire si la valeur saisie dans l'un des champs obligatoires d'une règle n'est pas valide (champ autre que le champ Description).

Solution : vérifiez que les éléments suivants sont corrects dans le fichier d'importation.

- Valeurs de champ : les définitions de règle comportent des valeurs de champ prises en charge. Les valeurs sont entrées correctement.
- Format : les colonnes correctes sont incluses dans le fichier. Les noms de colonne sont orthographiés correctement.

L'objet Mappage d'applications n'est pas valide : le champ d'IP ne peut pas être vide

L'erreur peut se produire si l'une des conditions suivantes est remplie :

- La valeur de l'ID d'application NBAR2 est manquante pour une règle NBAR2.
- La valeur d'adresse IP de serveur est manquante pour une règle Hôte (serveur).

Solution : ajoutez la valeur manquante à la définition de règle.

L'objet Mappage d'applications n'est pas valide : la valeur du masque doit être comprise entre 0 et 32

La règle Sous-réseau inclut une valeur de masque non prise en charge.

Solution : spécifiez une valeur de masque comprise entre 0 et 32.

L'objet Mappage d'applications n'est pas valide : la valeur du type de service doit être comprise entre 0 et 255

La règle Tout (Type de service, ToS) inclut une valeur de type de service non prise en charge.

Solution : spécifiez une valeur de type de service comprise entre 0 (tous les types de service) et 255.

Erreur : nom de paramètre manquant dans la liste -params

Un des champs obligatoire de la règle ne contient pas de valeur.

Solution : vérifiez que toutes les valeurs des champs obligatoires sont incluses. Toutes les valeurs de champ sont requises, sauf le champ Description.

Pour afficher l'aide de la commande, entrez :
`setapplicationmapping`

Utilisation des places réservées

Vous pouvez créer des règles de places réservées pour que les rapports incluent les combinaisons de port et de protocole qui vous intéressent, indépendamment du volume ou du taux de trafic. Les règles créent des places réservées pour les ports utilisés par ces protocoles, afin de garantir que les données sont incluses dans les rapports.

Par exemple, pendant un déploiement d'application, vous voulez consulter le trafic pour une application particulière, mais les rapports N principaux protocoles pour les interfaces n'affichent pas le trafic de l'application. Le protocole utilisé par l'application n'est pas inclus dans le groupe N principaux protocoles (groupe de protocoles affichant le volume de trafic ou d'utilisation le plus élevé). Vous créez une règle Places réservées pour collecter des données pour le protocole spécifique et le port utilisé par l'application. Le protocole est désormais inclus dans les rapports N principaux protocoles.

Remarque : Les données généralement collectées par CA Network Flow Analysis sont décrites dans la rubrique Procédure de collecte des données (page 188).

Création de règles de places réservées

Créez des règles de places réservées pour que les rapports incluent les combinaisons de port et de protocole qui vous intéressent, indépendamment du volume ou du taux de trafic.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche.

2. Dans la liste Règles, sélectionnez Places réservées.

   La page Définitions d'application bascule en mode Places réservées et affiche une liste des règles de places réservées actuelles.

3. Cliquez sur Ajouter une règle.

   La boîte de dialogue Ajouter des places réservées s'ouvre.

4. Spécifiez les ports de la manière suivante :

   ■ Protocole : protocole des données affecté par la règle (TCP ou UDP).

   ■ Port : port cible pour la règle de places réservées. Introduisez le numéro de port dans la zone Port, une valeur de 0 à 65535 exprimée au format décimal de base 10. Si vous n'entrez aucune valeur, le port 0 est affecté. L'association du port et du protocole doit être unique et ne doit correspondre à aucune autre règle de places réservées.

     Les données du type de protocole spécifié sont incluses dans les rapports pour ce port, indépendamment du volume ou du taux de trafic.

   ■ Description (facultatif) : texte d'identification pour la règle de places réservées. La description s'affiche dans la liste des règles de places réservées de la page Définitions d'application.

5. Cliquez sur Enregistrer.

   Si vous avez entré une combinaison port/protocole valide et que le nombre maximum de règles n'a pas été atteint, la boîte de dialogue se ferme. La nouvelle règle s'affiche dans la liste des règles de places réservées.

6. Répétez ce processus pour chaque règle de places réservées à ajouter.

   Vous pouvez spécifier un maximum de 50 règles de places réservées.

Modification de règles de places réservées

Modifiez une règle de places réservées pour appliquer des corrections au port, au protocole ou à la description spécifiée.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche.

2. Dans la liste Règles, sélectionnez Places réservées.

   La page Définitions d'application bascule en mode Places réservées et affiche une liste des règles de places réservées actuelles.

3. Cochez la case à côté de la règle que vous voulez modifier, puis cliquez sur Modifier.

   La boîte de dialogue Modifier des places réservées s'ouvre.

4. Effectuez les modifications requises pour les valeurs Protocole, Port et Description, puis cliquez sur Enregistrer.

   Si les modifications sont appliquées correctement, la boîte de dialogue se ferme.

Suppression de règles de places réservées

Supprimez des règles de places réservées lorsqu'elles sont obsolètes.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu Administration, sélectionnez Définitions d'application.

      La page Définitions d'application s'affiche.

2. Dans la liste Règles, sélectionnez Places réservées.

   La page Définitions d'application bascule en mode Places réservées et affiche une liste des règles de places réservées actuelles.

3. Cochez la case située à côté de la règle à supprimer. Pour sélectionner les cases à cocher pour toutes les règles, cochez la case à cocher de la ligne de titre.

4. Cliquez sur Supprimer.

   Un message de confirmation s'affiche.

5. Cliquez sur Oui.

   La liste des règles de places réservées est mise à jour pour refléter les suppressions.

Utilisation des priorités de port

Par défaut, CA Network Flow Analysis définit le port et le protocole du serveur sur le nombre le plus faible dans l'enregistrement de flux.

Port source : 80

Port de destination : 8000

Dans ce cas, NFA déduit que le port le plus faible est 80 et donc de type HTTP.

Vous pouvez utiliser la priorité de port lorsque le port de serveur (TCP/UDP) utilise un nombre élevé.

Par exemple :

Port de serveur : 8888

Port client : 6000

Par défaut, NFA utilise le port le plus faible (6000) comme port de serveur. La fonctionnalité Priorité du port indique à NFA d'utiliser le port 8888 comme port de serveur lorsqu'il est présent dans les données.

Création de règles de priorité du port

La création de règles de priorité du port garantit l'identification des protocoles appropriés pour chaque plage de ports.

Procédez comme suit :

1. Ouvrez la page **Définitions d'applications** :
    a. Dans le menu de console NFA, sélectionnez **Administration**. La page **Administration** s'ouvre.
    b. Dans le menu **Administration**, sélectionnez **Définitions d'applications**. La page **Définitions d'applications** s'affiche.
2. Dans la liste **Règles**, sélectionnez **Priorité du port**.

    La page **Définitions d'applications** bascule en mode **Priorité du port** et affiche une liste des règles de priorité de port actuelles.
3. Cliquez sur **Ajouter une règle**.

    La boîte de dialogue **Ajouter une priorité de port** s'ouvre.

4. Spécifiez les ports de la manière suivante :
   - Protocole : protocole des données affecté par la règle (TCP ou UDP).
   - **Port de début** : port de début cible pour la règle de priorité de port. Dans la zone Port de début, entrez le numéro du port. Il doit s'agir d'une valeur comprise entre 0 et 65 535 et exprimée au format décimal de base 10. Si vous n'entrez aucune valeur, le port 0 est affecté.
   - **Port de fin** : port de fin cible pour la règle de priorité de port. Dans la zone Port de fin, entrez le numéro du port. Il doit s'agir d'une valeur comprise entre 0 et 65 535 et exprimée au format décimal de base 10. Si vous n'entrez aucune valeur, le port 0 est affecté.

     Remarque : La combinaison de port de début, port de fin et protocole doit être unique, c'est-à-dire qu'elle ne doit correspondre à aucune autre règle de priorité de port.
   - **Description** (facultative) : texte d'identification de la règle de priorité de port. La description s'affiche dans la liste des règles de priorité de port de la page Définitions d'applications.
5. Cliquez sur **Save (Enregistrer)**.

   Si vous avez entré une combinaison port de début, port de fin et protocole valide et que le nombre maximum de règles n'a pas été atteint, la boîte de dialogue se ferme. La nouvelle règle s'affiche dans la liste des règles de priorité de port.
6. Répétez ce processus pour chaque règle de priorité de port à ajouter.

   Vous pouvez spécifier un maximum de 50 règles de priorité de port.

Configuration du clonage de flux

Vous pouvez utiliser la fonctionnalité Outil de clonage de flux pour transférer des données de flux à partir d'un Harvester compatible avec les flux vers une autre unité de collecte, par exemple un Harvester dans un déploiement différent. Par exemple, le Outil de clonage de flux peut envoyer des flux à un système de détection d'intrusions (IDS). Il permet d'envoyer les mêmes données vers deux unités de collecte sans surcharger vos routeurs avec le double envoi des données.

Une fois que vous avez installé et configuré le Outil de clonage de flux, les flux destinés au Harvester sont envoyés lorsque le service de clonage de flux CA NFA est lancé. Par défaut, le service démarre au redémarrage du serveur. Vous pouvez modifier ce comportement pour exécuter le service à la demande. Pour permettre au service de démarrer, le fichier de configuration doit identifier au moins une adresse IP de destination.

Le Outil de clonage de flux écoute les paquets en mode de proximité, puis les envoie aux adresses IP indiquées. Dans ce mode, le Outil de clonage de flux transmet les paquets à un autre processus qui les écoute. Un Harvester installé au même emplacement qu'un Outil de clonage de flux en cours d'exécution voit tous les paquets qui sont destinés à cet autre processus.

Installez le Outil de clonage de flux sur le serveur de Harvester dans un déploiement distribué ou sur le serveur unique dans un déploiement autonome.

Remarque : Le Outil de clonage de flux n'a affecté que très peu les performances du Harvester au cours des tests réalisés. Toutefois, si vous utilisez le Outil de clonage de flux sur un serveur de Harvester à flux élevé, nous vous recommandons de surveiller les performances.

Configuration requise pour l'installation de l'outil de clonage de flux

Avant d'installer Outil de clonage de flux, vérifiez que votre serveur d'installation satisfait les conditions préalables suivantes :

- La configuration et l'installation ou la mise à niveau du serveur respectent les conditions spécifiées dans le *Manuel d'installation de CA Network Flow Analysis* ou dans le *Manuel de mise à niveau de CA Network Flow Analysis.*
- Le logiciel a déjà été installé et configuré sur le serveur pour l'utiliser comme l'un des composants suivants :
  - Serveur de Harvester Windows dans un déploiement CA Network Flow Analysis 9.3.0 distribué
  - Serveur unique dans un déploiement autonome.
- Le serveur dispose de 12,8 Mo minimum d'espace de disque sur le lecteur cible pour le Outil de clonage de flux.
- Vous avez fermé tous les autres programmes.
- Aucun autre utilisateur n'est connecté au serveur.

Installation de l'outil de clonage de flux

Suivez la procédure détaillée dans cette rubrique pour installer Outil de clonage de flux.

Procédez comme suit :

1. Connectez-vous au serveur d'installation Harvester Windows en tant qu'utilisateur disposant de droits d'administrateur.

   Le serveur d'installation doit contenir le logiciel Harvester CA Network Flow Analysis 9.3.0.

2. Localisez le fichier du programme d'installation : <chemin_installation>\setup\FlowClonerSetup9.3.0.exe.

3. Lancez le programme d'installation : double-cliquez sur le fichier FlowClonerSetup9.3.0.exe dans l'explorateur Windows.

4. Dans la boîte de dialogue Bienvenue, cliquez sur Suivant.

   La fenêtre Récapitulatif de pré-installation s'ouvre et indique les conditions à suivre au niveau du chemin d'installation et en matière d'espace disque. Le Outil de clonage de flux sera installé dans le même répertoire d'installation racine que le Harvester ou le logiciel autonome.

5. Cliquez sur Installer.

   La fenêtre Fin de l'installation s'ouvre à l'issue de l'installation.

6. Cliquez sur Terminé.

   Le programme d'installation se ferme. Un fichier journal d'installation appelé FlowCloner_Install_<horodatage>.log est créé dans le répertoire d'installation racine.

Etape suivante : Configuration des options de l'outil de clonage de flux (page 151)

Configuration des options de l'outil de clonage de flux

Pour configurer le Outil de clonage de flux, modifiez son fichier d'initialisation par défaut (.ini). Le fichier INI contient une ligne d'en-tête suivie d'une ligne pour chaque hôte de destination (chaque hôte qui recevra les paquets clonés). Vous devez spécifier au moins un hôte de destination. Si vous n'entrez pas de valeurs pour les champs d'en-tête, les valeurs par défaut sont utilisées.

Pour plus d'informations sur les conventions du fichier de configuration, y compris sur la procédure à suivre pour commenter des lignes ou des champs, consultez la rubrique Conventions applicables aux fichiers de configuration de l'outil de clonage de flux (page 154).

Procédez comme suit :

1. Connectez-vous au serveur d'installation du Outil de clonage de flux en tant qu'utilisateur avec des droits d'administrateur.
2. Ouvrez le fichier suivant dans un éditeur de texte : <chemin_installation>\Netflow\FlowCloner\flowclonedef.ini.

   Le fichier INI inclut une ligne d'en-tête suivie d'une ligne pour chaque hôte qui recevra des paquets.
3. Personnalisez la ligne d'en-tête :

   Le contenu de l'en-tête doit figurer sur une seule ligne, la première ligne non commentée et non vide du fichier.

   - Pour utiliser la valeur par défaut pour le NIC d'entrée, remplacez la totalité de la ligne d'en-tête par le jeton suivant :

     ```
     /use defaults
     ```

     Vous pouvez faire suivre le jeton */use defaults* d'un commentaire, comme l'illustre l'exemple suivant :

     ```
     /use defaults ; use first available NIC and port 9995 to listen
     and send flows on the first available NIC
     ```

     Le programme utilise le premier NIC disponible. Les hôtes écoutent les flux d'origine et les flux clonés sur le port UDP 9995. Le jeton */use defaults* prend effet uniquement si l'en-tête ne contient pas d'autres jetons.
   - (Facultatif) Pour spécifier le port d'écoute, entrez le jeton /port= et faites-le suivre du numéro de port. Le Harvester qui reçoit les flux d'origine utilise le port UDP 9995 pour l'écoute, sauf si vous utilisez le jeton /port pour spécifier un autre port.

     Valeur par défaut : UDP 9995

- (Facultatif) Pour spécifier le port de destination, entrez le jeton /dest port= et faites-le suivre du numéro de port. Les hôtes qui reçoivent les flux clonés utilisent le port UDP 9995 pour l'écoute, sauf si vous utilisez le jeton /dest port pour spécifier un port différent. Tous les hôtes écoutent les flux clonés sur le même port.

  Valeur par défaut : UDP 9995

- (Facultatif) Pour spécifier le NIC d'entrée, entrez le jeton */listen ip=* et faites-le suivre de l'adresse IP du NIC sur lequel le Outil de clonage de flux écoute les paquets.

  Valeur par défaut : première adresse IP fonctionnelle de l'hôte

Pour consulter des exemples, reportez-vous à la rubrique Exemples de fichiers de configuration de l'outil de clonage de paquets de flux (page 153).

4. Spécifiez un ou plusieurs hôtes pour la réception des paquets clonés :

   Entrez chaque hôte sur une ligne distincte composée du jeton *dest ip=* et de l'adresse IP de l'hôte de destination. Aucun ordre n'est imposé au niveau des lignes de l'hôte de destination.

   Exemple :

   ```
   /dest ip=10.0.0.100 ; send cloned packets to 10.0.0.100
   ```

   Si une adresse IP est manquante, la ligne est ignorée.

5. Enregistrez et fermez le fichier FlowCloneDef.ini.

6. Lancez le service de clonage de flux CA NFA sur le serveur de Harvester.

   Le Outil de clonage de flux est activé et tente d'envoyer les paquets à chaque destination valide spécifiée. Le clonage de flux poursuit jusqu'à l'arrêt manuel du service de clonage de flux CA NFA.

   Le service de clonage de flux CA NFA est configuré pour commencer automatiquement l'envoi des données des flux clonés au redémarrage du serveur. Pour que le Outil de clonage de flux fonctionne uniquement à la demande, modifiez cette configuration dans la fenêtre Services. Vous pouvez par exemple exécuter le service uniquement si le fichier de configuration identifie au moins une adresse IP de destination.

Voir également :

- Exemples de fichiers de configuration de l'outil de clonage de flux (page 153)
- Conventions applicables aux fichiers de configuration de l'outil de clonage de flux (page 154)
- Caractéristiques des paquets clonés (page 154)

Exemples de fichiers de configuration de l'outil de clonage de flux

Les exemples suivants indiquent le contenu d'un fichier FlowCloneDef.ini modifié pour un serveur de NIC unique et pour un environnement de serveurs de NIC multiples.

Exemple : NIC et port d'entrée par défaut

Dans cet exemple, le Outil de clonage de flux utilise le premier NIC disponible pour envoyer les données clonées aux hôtes 192.100.0.100 et 192.160.0.100. Les hôtes de destination écoutent les données sur le port UDP 9995.

L'exemple inclut une ligne pour chaque hôte qui reçoit les données clonées. Ces lignes commencent par le jeton */dest ip=* suivi de l'adresse IP de l'hôte. Un point-virgule précède les commentaires en fin de ligne.

```
/use defaults; take default setup
/dest ip=192.100.0.100; send cloned packets to ddev1
/dest ip=192.160.0.100; send cloned packets to gdev3
```

Exemple : NIC et port d'entrée personnalisés

Dans cet exemple, le Outil de clonage de flux utilise un NIC spécifié (190.0.0.100) pour envoyer les données clonées aux hôtes (10.0.0.000, 192.100.0.100 et 192.160.0.100). Les Harvesters écoutent les données entrantes d'origine sur le port UDP 9994.

Remarque : Si vous spécifiez une valeur */port* personnalisée, elle doit correspondre au port d'écoute du Harvester et au port de destination que vous avez utilisés pour configurer le flux. Les valeurs de port doivent correspondre, sans quoi aucune donnée de flux n'est clonée.

```
/listen ip=190.0.0.100; Use 190.0.0.100 to send the cloned packets
/port=9994; Listen on port 9994 instead of the default port 9995
/dest ip=10.0.0.000 ; send cloned packets to 10.0.0.000
/dest ip=192.100.0.100; send cloned packets to ddev1
/dest ip=192.160.0.100; send cloned packets to gdev3
```

Exemple : NIC et port de destination personnalisés

Dans cet exemple, le Outil de clonage de flux utilise un NIC spécifié (190.0.0.100) pour envoyer les données clonées à l'hôte 10.0.0.000. Les Harvesters qui reçoivent les données clonées écoutent sur le port UDP 9996.

```
/listen ip=190.0.0.100; Use 190.0.0.100 to send the cloned packets
/dest port=9996; Listen for the cloned data on port 9996
/dest ip=10.0.0.000 ; send cloned packets to 10.0.0.000
```

Conventions applicables aux fichiers de configuration de l'outil de clonage de flux

Les fichiers FlowCloneDef.ini doivent respecter les conventions suivantes :

- Ligne d'en-tête : le fichier FlowCloneDef.ini doit commencer par une ligne unique, qui contient toutes les entrées de valeur de jeton d'en-tête.
- Lignes d'hôte de destination : faites suivre la ligne d'en-tête par une ligne pour chaque hôte de destination. Utilisez le format suivant /dest ip=<X.X.X.X>, où <X.X.X.X> correspond à l'adresse IP de l'hôte de destination. Aucun ordre n'est imposé au niveau des lignes d'hôte de destination, mais les lignes dest ip= doivent suivre la ligne d'en-tête.
- Jetons : faites précéder toutes les valeurs dans le fichier d'un jeton qui identifie le type de valeur définie. Faites précéder chaque jeton d'un caractère **|** ou **/** pour indiquer qu'un autre jeton lui succède.

  Les jetons sont ignorés dans les cas suivants :

  - Ils ne sont pas pris en charge.
  - Ils ne respectent pas les conditions de spécification.
  - Ils n'incluent aucune valeur.

  Le jeton */use defaults* est ignoré si la ligne d'en-tête contient également une ou plusieurs entrées de valeur de jeton.
- Pour commenter le contenu :
  - Ligne entière : entrez un point-virgule (**;**) au début de la ligne. La ligne entière est ignorée.
  - Contenu allant d'un point particulier au début du jeton suivant : entrez un point-virgule (**;**) au début du contenu à ignorer.
  - Ensemble du contenu inclus entre le point particulier et la fin de la ligne : entrez deux points-virgules (**;;**) au début du contenu à ignorer.

Caractéristiques des paquets clonés

Tous les paquets IP clonés possèdent les caractéristiques suivantes :

- Valeur ToS des paquets clonés = 0 (zéro), indépendamment de la valeur du paquet d'origine. Cette valeur caractérise la valeur ToS des paquets clonés qui contiennent les flux. Les valeurs ToS du trafic que les flux décrivent ne sont pas alternées.
- Leur port d'envoi est 10 000, quel que soit le port utilisé pour l'envoi du paquet d'origine.
- La durée de vie est définie sur 255, quelle que soit la valeur affectée à ce paramètre pour le paquet d'origine
- ID de fragment : numéro arbitraire

Chapitre 9: Maintenance et collecte des données

Effectuez des opérations de maintenance sur CA Network Flow Analysis pour un fonctionnement optimal des fonctionnalités. Vous souhaiterez effectuer certaines tâches de maintenance de façon périodique. Par exemple, lorsqu'un utilisateur configure une interruption, l'administrateur doit la déployer.

Remarque : Pour effectuer les tâches décrites dans cette rubrique, le rôle défini pour votre compte d'utilisateur de la console NFA doit être Administrateur ou Utilisateur avancé.

Affichage du statut du système

Affichez la page Statut du système pour vérifier le statut global des composants CA Network Flow Analysis.

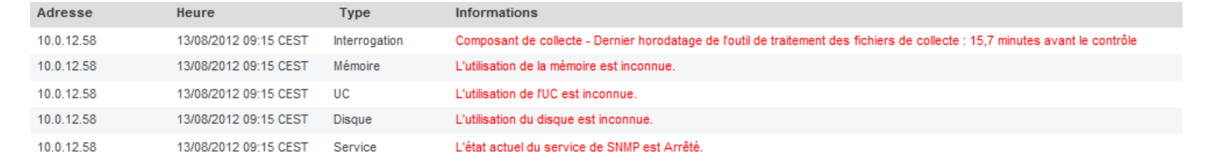
Procédez comme suit :

1. Affichez la page Statut du système :
   - Dans le menu de console NFA, sélectionnez Administration.

     ou
   - Dans le menu Administration, sélectionnez Statut du système.

   La page Statut du système s'ouvre et affiche un aperçu rapide du statut des composants CA Network Flow Analysis. Les symboles de statut identifient les composants pour lesquels des avertissements ont été générés. Le nombre d'avertissements s'affiche entre parenthèses après l'étiquette de composant.
2. Cliquez sur un composant affichant un symbole d'avertissement pour consulter les détails.

   Une table d'avertissements s'affiche.



Adresse	Heure	Type	Informations
10.0.12.58	13/08/2012 09:15 CEST	Interrogation	Composant de collecte - Dernier horodatage de l'outil de traitement des fichiers de collecte : 15,7 minutes avant le contrôle
10.0.12.58	13/08/2012 09:15 CEST	Mémoire	L'utilisation de la mémoire est inconnue.
10.0.12.58	13/08/2012 09:15 CEST	UC	L'utilisation de l'UC est inconnue.
10.0.12.58	13/08/2012 09:15 CEST	Disque	L'utilisation du disque est inconnue.
10.0.12.58	13/08/2012 09:15 CEST	Service	L'état actuel du service de SNMP est Arrêté.

3. Vérifiez chaque avertissement pour chaque composant.

Configuration des paramètres de l'application

La page Paramètres de l'application inclut de nombreux paramètres.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.

   La page Statut du système s'ouvre.

2. Dans le menu Administration situé à gauche, sélectionnez Administration, Système, puis Paramètres de l'application.

   La page Paramètres de l'application s'affiche.

3. (Facultatif) Modifiez les paramètres suivants si nécessaire et cliquez sur Enregistrer :

   Limite d'absence de données d'interface

   Spécifie la durée pendant laquelle le programme doit patienter avant de marquer une interface comme inactive, à compter de la valeur Dernier flux sur la page Interfaces disponibles. Lorsque la limite est atteinte, le statut de l'interface est modifié aux emplacements suivants :

   - Index d'interface : la valeur de la colonne Actif(ve) devient Non.
   - Page Interfaces actives : la valeur Statut du trafic devient Inactif(ve)/Rouge.

   Valeur par défaut : 4 heures

   Port de redirection TCP

   Spécifie le port cible du trafic TCP redirigé par une règle de mappage d'applications. Le trafic TCP qui ne doit pas accéder au port cible est transféré vers le port de redirection TCP. D'autres paramètres ont une incidence sur le comportement du mappage d'applications : Port de redirection UDP, Masque du type de service et Conserver le protocole de mappage ToS. Pour plus d'informations, consultez le contenu de la rubrique Configuration du mappage d'applications (page 122).

   Valeur par défaut : 9000

   Masque ToS

   Indique le nombre de bits que les règles de mappage d'applications utilisent pour la correspondance des valeurs de type de service. La valeur par défaut 255 indique au programme de rechercher des correspondances dans l'ensemble des valeurs de type de service. D'autres paramètres ont une incidence sur le comportement du mappage d'applications : Port de redirection TCP et Conserver le protocole de mappage ToS. Pour plus d'informations, consultez le contenu de la rubrique Configuration du mappage d'applications (page 122).

   Valeur par défaut : 255

Port de redirection UDP

Spécifie le port cible du trafic UDP redirigé par une règle de mappage d'applications. Le trafic UDP qui ne doit pas accéder au port cible est transféré vers le port de redirection UDP. D'autres paramètres ont une incidence sur le comportement du mappage d'applications : Port de redirection TCP, Masque du type de service et Conserver le protocole de mappage ToS. Pour plus d'informations, consultez le contenu de la rubrique Configuration du mappage d'applications (page 122).

Valeur par défaut : 8000

Interfaces Auto-Enable

Indique si les interfaces nouvellement détectées sont activées automatiquement (True) ou sont désactivées (False). Pour définir les interfaces pour lesquelles un rapport doit être généré et pour connaître les licences utilisées, vous pouvez définir la valeur sur False. Vous devez ensuite activer les interfaces manuellement à la page Interfaces disponibles (page 82). Ce paramètre affecte le statut Activé des nouvelles interfaces. Les modifications apportées à ce paramètre n'ont aucun impact sur les interfaces déjà détectées.

Valeur par défaut : True

Fuseau horaire par défaut

Définit le fuseau horaire des rapports personnalisés et d'analyse en cours d'exécution. Par exemple, le début et la fin du jour de la période de génération de rapports définie sur 1 jour pour un rapport personnalisé sont définis en fonction fuseau horaire par défaut. Le fuseau horaire de l'opérateur qui exécute le rapport n'est pas utilisé.

Valeur par défaut : GMT

Domaines DNS

Supprime les suffixes spécifiés dans les noms d'hôte des vues et des rapports de la console NFA. Si vous incluez .mon_entreprise.com, par exemple, ce suffixe n'apparaît pas dans les noms d'hôte des vues et des rapports. Pour spécifier plusieurs entrées, séparez-les à l'aide d'une virgule et sans insérer d'espaces.

Valeur par défaut : <aucune valeur par défaut>

Afficher les zéros de la ligne de tendance

Spécifie si les rapports de ligne de tendance doivent indiquer les données avec des lignes d'interconnexion.

Si la valeur est True, les lignes de tendance connectent les points de données dans les rapports de type Récapitulatif des tendances multiples et Tendance empilée, sur les pages Interface. Le modèle de remplissage est indiqué en dessous des lignes.

Si la valeur est False, les rapports indiquent uniquement les points de données réels. La ligne de tendance finit au dernier point de données et commence au point de données suivant. Les rapports présentent des valeurs vides lorsque des points de données sont manquants. Le modèle de remplissage est manquant, car les rapports n'incluent pas de lignes de limite pour ce type de modèle.

Valeur par défaut : False

Adresse de l'expéditeur

Spécifie l'adresse électronique de l'administrateur NFA insérée dans le champ De lorsqu'un rapport est envoyé par courriel. Si ce paramètre n'est pas configuré, les utilisateurs ne peuvent pas envoyer de rapports planifiés ou immédiats. Ces fonctions requièrent également la configuration d'une valeur de serveur SMTP.

Valeur par défaut : <aucune valeur par défaut>

SMTP Server (Serveur JDBC)

Spécifie l'adresse IP du serveur de messagerie SMTP utilisée pour envoyer des rapports par courriel. Si ce paramètre n'est pas configuré, les utilisateurs ne peuvent pas envoyer de rapports planifiés ou immédiats. Ces fonctions requièrent également la configuration d'une valeur Adresse de l'expéditeur.

Valeur par défaut : <aucune valeur par défaut>

Unités avec licence

Enregistre le nombre total de licences que vous avez achetées auprès de CA. Cette valeur est utilisée pour calculer le pourcentage de licences en cours d'utilisation, qui est affiché à la page A propos de. Le pourcentage d'utilisation de la licence est précis uniquement si la valeur Unités avec licence l'est elle aussi.

Valeur par défaut : 50

Conserver le protocole de mappage ToS

Spécifie si le trafic de protocole pour les données mappées par application et basées sur le type de service est combiné (N) ou est affiché en tant que flux de données distincts étiquetés avec les indicateurs de protocole d'origine (Y).

Par exemple, imaginons que la valeur est Y et que vous mappez le trafic de protocole TCP, UDP ou tout autre trafic de protocole IP vers un port. Pour notre exemple toujours, supposons que vous accédez à un lien dans la vue Présentation d'Entreprise : Principaux hôtes pour un hôte auquel des données sont mappées. Dans ce cas, les vues Tendance empilée des protocoles et Tendance des protocoles sont visibles et indiquent si le trafic de protocole est de type TCP, UDP ou concerne un autre protocole IP.*

Si la valeur Conserver le protocole de mappage ToS est N et si les vues Tendance de empilée des protocoles indiquent le trafic de protocole associé, tous les protocoles pour le trafic mappé sont combinés dans un flux de trafic unique auquel une étiquette TCP est affectée.

* Les vues Tendance empilée des protocoles et Tendance des protocoles indiquent le trafic de protocole qui remplit les conditions suivantes : (1) Le trafic dépasse le seuil minimum et (2) Le volume de protocole est suffisamment élevé pour placer le protocole dans le groupe N principaux.

D'autres paramètres ont une incidence sur le comportement du mappage d'applications : Port de redirection TCP, Port de redirection UDP et Masque du type de service. Pour plus d'informations, consultez le contenu de la rubrique Configuration du mappage d'applications (page 122).

Valeur par défaut : Y

Pompage de l'émission ou de la multidiffusion

Spécifie si les vues et les rapports d'interface incluent (True) ou masquent (False) le trafic de diffusion ou de multidiffusion.

Valeur par défaut : True

IP du générateur de rapports

Spécifie l'adresse IP de l'unité ou de la console NFA. Le DSA dans un déploiement distribué à 3 niveaux utilise cette adresse IP pour contacter la console NFA. Si le paramètre est incorrect, le DSA ne peut pas récupérer les fichiers de données et vos rapports ne peuvent pas afficher de données de résolution en 15 minutes.

Valeur par défaut :

- Déploiement autonome : adresse IP de bouclage du serveur autonome
- Déploiement à 2 niveaux distribué (sans DSA) : adresse IP de bouclage de la console NFA
- Déploiement à 3 niveaux distribué : une fois que vous avez ajouté un DSA et répondu à l'invite de vérification de l'adresse IP de la console NFA, le programme met à jour l'adresse IP du générateur de rapports pour qu'elle corresponde à l'adresse IP de la console NFA.

Retard d'interrogation du service de rapport

Spécifie le nombre de secondes entre chaque contrôle de finalisation des rapports. Le statut Terminé(e) s'affiche lorsque les deux conditions suivantes sont remplies :

- Le contrôle de service de rapport confirme que le rapport est terminé.
- Vous actualisez la liste de rapports sur la page Génération de rapports personnalisés, Analyse ou Examen des flux.

Valeur par défaut : 15

Domaines du routeur

Supprime les suffixes spécifiés des noms de routeur qui s'affichent dans les vues et les rapports de la console NFA. Pour spécifier plusieurs entrées, séparez-les à l'aide d'une virgule et sans insérer d'espaces.

Valeur par défaut : <aucune valeur par défaut>

Afficher les agrégations

Spécifie si les agrégations d'interface doivent être incluses dans des vues de page Présentation de l'entreprise. Si la valeur est True, les agrégations d'interface sont incluses dans les vues.* Les agrégations à inclure dans les vues de page Présentation de l'entreprise doivent présenter le trafic suffisant pour dépasser les seuils minimum et pour être classées dans le groupe N principaux.

Valeur par défaut : False

Afficher le nom de l'unité

Spécifie si le format de nom d'interface commence par le nom d'unité (True) ou l'ignore (False). Ce paramètre affecte les noms d'interface qui apparaissent dans les vues et les rapports, notamment dans les vues Présentation de l'entreprise, dans les rapports de page Interface et dans les Récapitulatifs personnalisés d'interface de rapport. Pour plus d'informations, consultez la rubrique Modification du paramètre de l'application pour les noms d'interface (page 87).

Valeur par défaut : True

Afficher le champ Commentaires

Affiche (True) ou masque (False) l'icône Notes pour les lignes d'interface de la page Interfaces actives. Si l'icône Notes est visible, vous pouvez cliquer dessus pour ajouter, modifier ou afficher des informations supplémentaires concernant une interface, comme décrit dans la rubrique Interfaces actives : informations sur les interfaces (page 64).

Valeur par défaut : False

Destination des interruptions

Adresse IP ou nom DNS du serveur cible pour l'envoi des interruptions affichées comme des événements dans la console Performance Center, à la page Affichage des événements (CA PC) ou Liste des événements (NPC). Vous pouvez afficher des interruptions uniquement sous forme d'événements lorsque ce paramètre est configuré. Définissez la valeur de destination des interruptions de sorte qu'elle corresponde à l'adresse IP d'un des serveurs suivants :

- (CA PC) Console NFA ou serveur autonome enregistrés comme source de données auprès de Performance Center
- (NPC) Serveur du gestionnaire d'événements

Pour plus d'informations, reportez-vous à la rubrique Configuration de destinations des interruptions (page 168).

Valeur par défaut : adresse IP de la console NFA (déploiement distribué) ou du serveur autonome (déploiement autonome)

Procédure de surveillance des composants

Les services de surveillance vous permettent de surveiller les composants CA Network Flow Analysis. Les services de surveillance interrogent chaque serveur présents dans votre configuration CA Network Flow Analysis toutes les deux heures pour déterminer le statut de tous les composants. Vous pouvez établir des seuils, une adresse électronique pour la réception de messages et configurer d'autres paramètres pour que les services de surveillance vous notifie des problèmes rencontrés sur les composants dans les plus brefs délais.

Remarque : Pour obtenir des informations supplémentaires sur les services inclus sur chaque serveur de votre configuration CA Network Flow Analysis, consultez la rubrique Gestion des services (page 173).

Modification des paramètres du service de surveillance

Modifiez les paramètres de l'outil de surveillance pour modifier les valeurs de configuration comme les seuils, les paramètres d'interruption, les paramètres d'interrogation, l'adresse de notification et les chaînes de communauté.

Procédez comme suit :

1. Affichez la page Paramètres de l'outil de surveillance :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu de la page Administration, sélectionnez Intégrité : Paramètres de l'outil de surveillance.

      La page de Paramètres de l'outil de surveillance s'ouvre et affiche les paramètres actuels.

2. Modifiez les paramètres du service de surveillance :

   Chaîne de communauté

   Chaîne SNMP que les services de surveillance utilisent pour vérifier l'identité des composants inclus dans un déploiement distribué. La chaîne de communauté est utilisée pour la collecte d'informations à partir des Harvesters (et à partir de DSA dans un déploiement d'architecture à trois niveaux). Utilisez le même nom de communauté tout au long du déploiement de CA Network Flow Analysis :

   - Paramètres de l'outil de surveillance, page
   - Service SNMP sur chaque serveur Windows
   - Fichier snmpd.conf sur chaque serveur Linux

   Par défaut : public

Seuil d'UC

Seuil d'utilisation de l'UC. Si l'adresse et la chaîne sont définies, vous recevez un courriel lorsque le seuil d'UC d'un serveur est dépassé et une notification d'interruption SNMP est générée.

Par défaut : 80 % d'utilisation de l'UC

Seuil du disque

Seuil d'utilisation du disque. Si l'adresse et la chaîne sont définies, vous recevez un courriel lorsque le seuil de disque d'un serveur est dépassé et une notification d'interruption SNMP est générée.

Par défaut : 80 % d'utilisation du disque

Adresse électronique

Adresse électronique du destinataire à utiliser pour les notifications en cas de dépassement des seuils. Pour informer plusieurs destinataires, séparez les adresses par des virgules. Le paramètre Adresse électronique n'a aucune valeur par défaut.

Par défaut : (aucun)

Seuil de la mémoire

Seuil d'utilisation de la mémoire. Si l'adresse et la chaîne sont définies, vous recevez un courriel lorsque le seuil de mémoire d'un serveur est dépassé.

Par défaut : 80 % d'utilisation de la mémoire

Nouvelles tentatives SNMP

Nombre de tentatives d'interrogation d'une unité SNMP. Selon la configuration de votre réseau, un nombre élevé de tentatives SNMP peut affecter les performances.

Par défaut : 2

Délai d'expiration SNMP

Nombre de secondes avant l'expiration d'une interrogation SNMP.

Par défaut : 5

Intervalle de contrôle du système

Nombre de minutes entre les vérifications du système par l'outil de surveillance.

Par défaut : 60

Chaîne de communauté d'interruptions

Chaîne SNMP à utiliser pour l'envoi d'interruptions à un récepteur d'interruptions tiers. Utilisez l'un des noms de communauté que le récepteur d'interruptions doit accepter, conformément à sa configuration.

Par défaut : public

Destination des interruptions

Adresse IP du serveur recevant les interruptions SNMP à partir des services d'outil de surveillance. Les interruptions sont générées lorsque des violations de seuil des performances des composants CA Network Flow Analysis se produisent.

Par défaut : (aucun)

3. Lorsque vous avez modifiez les paramètres, cliquez sur Enregistrer.

Utilisation des interruptions

Créez des interruptions pour informer les gestionnaires de réseau lorsque certains événements se produisent. Les administrateurs peuvent créer des interruptions et doivent déployer toutes les interruptions créées par les utilisateurs.

Vous pouvez intégrer des interruptions CA Network Flow Analysis à des packages de gestion des pannes externes (page 170).

Création d'interruptions

Procédez comme suit :

1. Affichez la page Ajouter une définition d'interruption :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu de la page Administration, sélectionnez Alertes.

      La page Configuration des interruptions s'ouvre et affiche la liste des interruptions actuelles.
   c. Cliquez sur Ajouter.

      La page Ajouter une définition d'interruption s'ouvre.

2. Saisissez une description et définissez les interfaces que l'interruption surveille :
   - Description : identifie la nouvelle interruption. Saisissez des informations sur le protocole et le seuil, comme Surveillance de l'utilisation de Microsoft SQL au-dessus de 65%.
   - Sélectionner une interface ou Sélectionner un groupe d'interfaces : lien vers un index d'interfaces ou de groupes d'interfaces, que vous utilisez pour sélectionner les interfaces surveillées par l'interruption.

     Remarque : Si l'interface ou le groupe d'interfaces associé est supprimé après le déploiement de l'interruption, une erreur Groupe d'interfaces inconnu se produira. Pour éliminer cette erreur, associez l'interruption à une interface ou à un groupe d'interfaces différent.
3. (Facultatif) Créez une interruption basée sur l'utilisation en fournissant les informations suivantes :
   - Seuils : Utilisation : permet de définir le type de seuil de l'interruption sur l'utilisation. Utilisez les champs contextuels qui sont ajoutés pour ce type d'interruption.
   - Champ Utilisation : En entrée : pourcentage de l'utilisation qui correspond à la valeur de seuil en entrée.
   - Liste Utilisation : En entrée : Minutes : nombre de minutes pour la violation de seuil en entrée qui génère une interruption.
   - Champ Utilisation : En sortie : pourcentage de l'utilisation qui correspond à la valeur de seuil en sortie.
   - Liste Utilisation : En sortie : Minutes : nombre de minutes pour la violation de seuil en sortie qui génère une interruption.
   - Protocole : protocole pour le trafic surveillé. Dans la boîte de dialogue Index de protocole qui s'ouvre, sélectionnez le protocole. L'interruption s'appliquera au protocole et aux interfaces sélectionnées.
   - Type de service (facultatif) : type de service (ToS) du trafic surveillé. L'interruption s'appliquera aux interfaces, au protocole et au type de service sélectionnés. Pour surveiller l'ensemble du trafic des différents types de service, sélectionnez Tout.
   - Filtre de temps (facultatif) : période de la surveillance, si vous choisissez de la limiter de cette façon. Sélectionnez un des filtres de temps de la liste. La liste Filtre de temps inclut tous les filtres de temps créés par l'administrateur.

4. (Facultatif) Créez une interruption basée sur le taux en fournissant les informations suivantes :

   Par exemple, vous créez une interruption basée sur le taux et établissez des seuils aussi bien pour le trafic entrant que pour le trafic sortant. L'interruption est déclenchée lorsque le seuil est dépassé lors de la période définie.

   - Seuils : Débit : permet de définir le seuil de l'interruption sur le taux de transfert des données. Utilisez les champs contextuels qui sont ajoutés pour ce type d'interruption.
   - Taux : En entrée : vitesse de transfert des données en entrée qui correspond à la valeur de seuil. Définissez le nombre de bits, de kilobits, de mégabits ou de gigabits par seconde, en fonction de l'unité de mesure sélectionnée.
   - Taux : Unités de mesure : unité de mesure pour le transfert de données. Sélectionnez Bits par seconde (bits/s), Kilobits par seconde (Kbits/s), Mégabits par seconde (Mbits/s) ou Gigabits par seconde (Gbits/s).
   - Taux : En entrée : Minutes : nombre de minutes pour la violation de seuil en entrée qui génère une interruption.
   - Taux : En sortie : seuil pour le transfert de données en sortie. Entrez le nombre de bits, de kilobits, de mégabits ou de gigabits par seconde, en fonction de l'unité de mesure sélectionnée pour le seuil en entrée.
   - Taux : En sortie: Minutes : nombre de minutes pour la violation de seuil en sortie qui génère une interruption.
   - Protocole : protocole pour le trafic surveillé. Dans la boîte de dialogue Index de protocole qui s'ouvre, sélectionnez le protocole. L'interruption s'appliquera au protocole et aux interfaces sélectionnées.
   - Type de service (facultatif) : type de service (ToS) du trafic surveillé. L'interruption s'appliquera aux interfaces, au protocole et au type de service sélectionnés. Pour surveiller l'ensemble du trafic des différents types de service, sélectionnez Tout.
   - Filtre de temps (facultatif) : période de la surveillance, si vous choisissez de la limiter de cette façon. Sélectionnez un des filtres de temps de la liste. La liste Filtre de temps inclut tous les filtres de temps créés par l'administrateur.

5. (Facultatif) Créez une interruption basée sur le volume en fournissant les informations suivantes :

   - Seuils : Volume : permet de définir le seuil de l'interruption sur le volume de données. Utilisez les champs contextuels qui sont ajoutés pour ce type d'interruption.
   - Volume : En entrée : volume de données en entrée qui correspond à la valeur de seuil. Définissez le nombre d'octets, de kilo-octets, de mégaoctets ou de gigaoctets, en fonction de l'unité de mesure sélectionnée.

- Volume : Unités de mesure : unité de mesure pour le transfert de données. Sélectionnez Octets, Kilo-octets (ko), Mégaoctets (Mo), Gigaoctets (Go) ou Téraoctets (To).
- Volume : En sortie : volume de données en sortie qui correspond à la valeur de seuil. Entrez le nombre d'octets, de kilo-octets, de mégaoctets ou de gigaoctets, en fonction de l'unité de mesure sélectionnée pour le seuil en entrée.
- Volume : En sortie: Minutes : nombre de minutes pour la violation de seuil en sortie qui génère une interruption.
- Protocole : protocole pour le trafic surveillé. Dans la boîte de dialogue Index de protocole qui s'ouvre, sélectionnez le protocole. L'interruption s'appliquera au protocole et aux interfaces sélectionnées.
- Type de service (facultatif) : type de service (ToS) du trafic surveillé. L'interruption s'appliquera aux interfaces, au protocole et au type de service sélectionnés. Pour surveiller l'ensemble du trafic des différents types de service, sélectionnez Tout.
- Filtre de temps (facultatif) : période de la surveillance, si vous choisissez de la limiter de cette façon. Sélectionnez un des filtres de temps de la liste. La liste Filtre de temps inclut tous les filtres de temps créés par l'administrateur.

6. (Facultatif) Créez une interruption basée sur le flux en fournissant les informations suivantes :
   - Seuils : Flux : permet de définir le seuil de l'interruption sur le nombre de flux. Utilisez les champs contextuels qui sont ajoutés pour ce type d'interruption.
   - Flux : Total : nombre de flux entrants qui correspond à la valeur de seuil. Définissez le nombre de flux par minute (unités, milliers, millions, etc.) selon l'unité de mesure sélectionnée.
   - Flux : Unités de mesure : unité de mesure pour le transfert de données. Sélectionnez Flux/minute, Milliers de flux/minute ou Millions de flux/minute.
   - Flux : Minutes : nombre de minutes pour la violation de seuil qui génère une interruption.
   - Filtre de temps (facultatif) : période de la surveillance, si vous choisissez de la limiter de cette façon. Sélectionnez un des filtres de temps de la liste. La liste Filtre de temps inclut tous les filtres de temps créés par l'administrateur.

7. Lorsque vous avez effectué vos sélections, cliquez sur Soumettre.

   L'interruption est déployée.

   Remarque : Les interruptions sont envoyées à la destination définie dans les paramètres d'application.

Pour supprimer une définition d'interruption, cliquez sur sa description dans la liste des interruptions de la page Configuration des interruptions. Cliquez sur le bouton Supprimer qui s'affiche en mode Modifier. Vérifiez la suppression lorsque vous y êtes invité.

Pour modifier une définition d'interruption, cliquez sur sa description dans la liste des interruptions de la page Configuration des interruptions. Effectuez les mises à jour dans la page Configuration des interruptions en mode Modifier. Cliquez sur Soumettre. L'interruption est mise à jour.

Configuration de destinations des interruptions

Configurez les destinations des interruptions créées (page 164) par vous et par les opérateurs.

- Définissez la destination des interruptions dans la page Paramètres de l'application pour afficher les interruptions comme des événements dans la console Performance Center.
- Si vous voulez également générer des interruptions de l'outil de surveillance, configurez la destination des interruptions dans la page Paramètres de l'outil de surveillance de la console NFA.

Pour activer l'affichage des interruptions dans la console Performance Center, procédez comme suit :

1. Affichez la page Paramètres de l'application :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu situé à gauche, sélectionnez Paramètres de l'application.

      La page Paramètres de l'application s'ouvre.

2. Recherchez le champ Destination des interruptions au bas de la page.
3. Vérifiez que la valeur du champ Destination des interruptions au bas des pages indique l'adresse IP appropriée :
   - (CA PC) Console NFA ou serveur autonome enregistrés comme source de données
   - (NPC) Serveur du gestionnaire d'événements

Pour connaître cette valeur dans CA Performance Center, assurez-vous que l'adresse IP dans le champ Destination des interruptions correspond à la valeur Nom de l'hôte dans CA Performance Center. Si l'adresse IP de l'hôte n'est pas incluse dans le nom de la source de données, vérifiez la valeur du paramètre Nom de l'hôte en procédant comme suit :

a. Dans la console Performance Center, sélectionnez Administration, puis Sources de données.

   La page Gérer les sources de données s'affiche.

b. Cliquez avec le bouton droit de la souris sur la source de données CA Network Flow Analysis et, dans le menu, sélectionnez Modifier.

   La boîte de dialogue Modifier la source des données s'ouvre.

c. Vérifiez la valeur du champ Nom de l'hôte.

Pour définir la destination des interruptions de l'outil de surveillance, procédez comme suit :

1. Affichez la page Paramètres de l'outil de surveillance :

   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.

   b. Dans le menu situé à gauche, sélectionnez Paramètres de l'outil de surveillance.

      La page de Paramètres de l'outil de surveillance s'ouvre et affiche les paramètres actuels.

2. Vérifiez que les paramètres de l'outil de surveillance sont corrects, y compris la destination des interruptions :

   Saisissez l'adresse IP du serveur qui héberge le récepteur d'interruptions. Les services de surveillance envoient des interruptions SNMP à l'adresse de destination des interruptions.

   Pour plus d'informations sur les autres paramètres de l'outil de surveillance, reportez-vous à la rubrique Modification des paramètres du service de surveillance (page 162).

3. Lorsque vous avez modifiez les paramètres, cliquez sur Enregistrer.

   Les paramètres sont enregistrés. Les messages seront envoyés pour toute nouvelle interruption générée.

Tâches facultatives :

- Vérifiez que les événements s'affichent dans la page Affichage des événements (CA PC) ou Event List (Liste des événements) (NPC). Si la page Affichage des événements ne montre pas les événements comme prévu, vérifiez que les conditions suivantes sont remplies :
  - Les journaux indiquent que les événements ont été générés et envoyés au gestionnaire d'événements.
  - Le nom d'hôte du gestionnaire d'événements peut être résolu par le serveur DNS pour CA Network Flow Analysis.
  - Dans la page Paramètres de l'application de la console NFA, la valeur du paramètre Destination des interruptions correspond à l'adresse IP du serveur de la console NFA ou du serveur autonome enregistré en tant que source de données.
- Configuration d'interruptions pour les programmes externes (page 171)

Procédure de configuration des interruptions pour les programmes externes de gestion des pannes

Vous pouvez intégrer les interruptions que CA Network Flow Analysis génère à l'aide d'autres programmes de gestion de réseau. Les interruptions fournissent les informations suivantes, qui peuvent être utiles dans d'autres programmes :

- L'interface affectée par le seuil
- Le protocole affecté par le seuil
- La direction du trafic affecté par le seuil (entrée, sortie ou les deux)
- Le seuil dépassé (par exemple, 1,23 Mo/s)
- Le trafic réel observé qui a déclenché l'interruption (par exemple, 1,30 Mo/s).
- Si la notification indique une nouvelle violation de seuil observée ou une violation de seuil effacée. Pour une violation de seuil effacée, le motif de l'effacement est inclus. Les motifs sont :
  - Le taux est retombé en dessous du seuil.
  - Aucune donnée n'a été détectée au cours de la dernière période.
  - Un filtre de temps a empêché l'inclusion des données.

Configuration d'interruptions pour les programmes externes

Configurez des interruptions CA Network Flow Analysis pour regrouper des événements dans les programmes externes et leur fournir des données utiles.

Procédez comme suit :

1. Accédez au fichier MIB.

   La base de données d'informations de gestion (MIB) contient les informations relatives au contenu des interruptions envoyées par CA Network Flow Analysis. Le fichier MIB se trouve dans le répertoire suivant : <chemin_installation>\reporter\MIB.

2. Compilez la base de données MIB dans votre programme de gestion de réseau et configurez ce dernier de façon à ce qu'il identifie les interruptions CA Network Flow Analysis de manière logique.

   Une interruption est envoyée lorsque le programme détecte une nouvelle violation de seuil et lorsque la condition est effacée. Configurez votre programme de gestion de réseaux pour regrouper ces deux événements, de façon à supprimer la condition d'avertissement lorsque le programme envoie l'interruption de condition d'effacement. Pour effectuer le regroupement, configurez le programme pour qu'il vérifie les valeurs suivantes dans la base de données d'informations de gestion :

   - NetQoSTrafficFlowEntry
   - NetQoSTrafficFlowDataEventStart, qui indique une nouvelle interruption.
   - NetQoSTrafficFlowDataEventStop, qui indique que l'interruption a été effacée.

   Pour plus d'informations sur la définition des règles pour le traitement intelligent des interruptions, consultez la documentation relative au programme de gestion de réseau.

3. Créez et déployez des interruptions CA Network Flow Analysis, si vous ne l'avez pas déjà fait, comme décrit dans la section Création d'interruptions (page 164).

4. Vérifiez que la destination d'interruption contient l'adresse IP du serveur qui héberge le programme de gestion des pannes.

   Les interruptions sont envoyées à la destination définie à la page Paramètres de l'application.

Dépannage des problèmes liés aux interruptions intégrées

Vérifiez les paramètres d'interruption pour corriger les problèmes rencontrés au niveau des données d'interruption CA Network Flow Analysis reçues par les programmes externes de gestion des pannes.

Procédez comme suit :

1. Vérifiez que la destination de l'interruption est définie sur l'adresse IP du serveur hôte du programme de gestion des pannes.
2. Vérifiez que les interruptions sont configurées correctement. Pour plus d'informations, consultez la rubrique Création d'interruptions (page 164).

Si vous avez vérifié ces paramètres, mais qu'aucune interruption n'est reçue comme prévu, contactez le support CA pour obtenir de l'aide.

Expiration des adresses caduques

Les adresses IP peuvent automatiquement être affectées à l'aide du protocole DHCP et peuvent expirées. Vous pouvez définir l'expiration d'adresses IP caduques (obsolètes) pour planifier leur actualisation. Vous pouvez également modifier la fréquence des mises à jour de nom DNS lorsque vous modifiez une adresse.

Le programme vérifie le serveur DNS et actualise le nom DNS pour chaque adresse expirée.

Procédez comme suit :

1. Affichez la page Configuration de l'adresse ou du nom d'hôte :
   a. Dans le menu de console NFA, sélectionnez Administration.

      La page Administration s'ouvre.
   b. Dans le menu de la page Administration, sélectionnez Génération de rapports : Adresses.

      La page Configuration de l'adresse ou du nom d'hôte s'ouvre :
2. (Environnement à domaines multiples uniquement) Sélectionnez la combinaison client hébergé/domaine qui contient l'adresse à actualiser.
3. Cliquez sur Liste.

   Une liste des adresses s'ouvre.

4. Cochez la case située à côté de chaque adresse que vous voulez marquer comme expirée.

5. Cliquez sur Expirer, puis confirmer l'expiration lorsque l'invite s'ouvre.

   L'actualisation de la résolution DNS des adresses sélectionnées est planifiée. Le processus d'actualisation est généralement exécuté dans les 5 minutes.

Gestion des services

Pour lancer ou arrêter des services et pour vérifier leur statut, vous pouvez utiliser les fenêtres Services Windows ou Configuration des services Linux.

Les services CA Network Flow Analysis et CA Anomaly Detector sont décrits brièvement dans la liste suivante. La colonne Autonome indique les services qui résident sur un serveur autonome à deux niveaux. Les autres colonnes de serveur indiquent où les services résident dans un déploiement distribué à deux ou à trois niveaux. Les services CA Anomaly Detector sont exécutés sur le serveur d'installation pour ce programme, qui peut être le serveur autonome, la console NFA ou le serveur CA Anomaly Detector distinct.

Service	**Autonome**	**Harvester**	**Console**	**DSA**	**Anomaly Detector**
Services Web de collecte et d'interrogation de CA NFA (Linux : nfa_collpollws) Fournit des interfaces de service Web rendant possible la communication entre la console NFA et le Harvester ou l'interrogateur (serveurs autonomes ou de Harvester).	Oui	Oui			
Conservation de données CA NFA (Linux : nfa_dataretention) Gère la suppression de caractères pour appliquer des limites de volume et de date à la conservation des fichiers de données. A 2 niveaux : données de résolution en 15 minutes, en 1 minute et d'examen des flux (serveur autonome/Harvester) A 3 niveaux : données de résolution en 15 minutes sur les serveurs DSA, en 1 minute et d'examen des flux sur les serveurs de Harvester	Oui	Oui		Oui	
Proxys DNS/SNMP CA NFA (Linux : nfa_proxies) Gère les demandes SNMP et DNS envoyées par l'interrogateur. Utilise le port 8081 par défaut.	Oui	Oui			

Service	**Autonome**	**Harvester**	**Console**	**DSA**	**Anomaly Detector**
CA NFA DSALoader A 3 niveaux : transforme les données de résolution en 15 minutes (fichiers .rpr) en fichiers .rpa15 devant être stockés sur des serveurs de DSA.				Oui	
Serveur de fichiers CA NFA (Linux : nfa_filewebservice) A 2 niveaux : dans un déploiement distribué, héberge le service Web sur les Harvesters pour gérer les demandes de fichier émises à partir du service de pompage de la console NFA. A 3 niveaux : héberge le service Web pour demander des transferts de fichiers entre les serveurs de DSA et de console NFA.	Oui	Oui	Oui (à 3 niveaux)		
Harvester CA NFA (Linux : nfa_harvester) Exécute le Harvester/processus de collecte.	Oui	Oui			
Service de solveur d'hôte CA NFA Recherche le nom de tous les hôtes pour lesquels une anomalie a été détectée par CA Anomaly Detector.	Oui				Oui
Service de suivi CA NFA Démarre et arrête le processus AnomalyDetector pour CA Anomaly Detector.	Oui				Oui
Interrogateur CA NFA (Linux : nfa_poller) Initialise et gère les demandes SNMP au niveau des unités qui exportent le flux vers le produit.	Oui	Oui			
Service de pompage CA NFA A 3 niveaux : récupère les fichiers .rpr à partir de la console NFA.				Oui	
Reaper CA NFA (Linux : nfa_reaper) Exécute le processus du Reaper, qui traite les fichiers entrants et écrit les fichiers sortants pour les données de résolution en 1 ou en 15 minutes ainsi que pour les données de présentation de l'entreprise.	Oui	Oui			

Service	Autonome	Harvester	Console	DSA	Anomaly Detector
Source de la base d'informations de génération de rapports de CA NFA Fournit une interface statique (interface de base de données des informations de rapports) pour l'affichage des données NFA qui apparaissent dans les vues Performance Center.	Oui		Oui		Oui
Authentification unique CA Performance Center Exécute le logiciel d'authentification unique, qui permet aux utilisateurs de passer de la console NFA à Performance Center et inversement, sans avoir à se réauthentifier.	Oui		Oui		
NetQoS MySql Exécute l'instance MySQL standard sur le port 3308 et stocke les données de configuration MySQL.	Oui	Oui	Oui	Oui	Oui
NetQoS NQMySql (Linux : nfa_mysqlCSE) Exécute les moteurs de stockage personnalisés et fournit une interface pour exécuter des requêtes de résolution en 1 ou en 15 minutes, ainsi que pour les données d'examen des flux.	Oui	Oui		Oui	
Service de gestionnaire de NetQoS Reporter Exécute les threads de maintenance en arrière-plan pour gérer l'interopération des composants.	Oui		Oui		
Services généraux de NetQoS Reporter/Analyzer Conservent les journaux dans le répertoire reporter/Logs et les données de présentation de l'entreprise.	Oui		Oui		
Service de pompage de NetQoS Reporter/Analyzer Tâches incluses : Collecte et traitement des données de présentation de l'entreprise provenant des Harvesters A 3 niveaux : collecte également les fichiers .rpr provenant des Harvesters et les copie dans un dossier simulé devant être récupéré par un DSA.	Oui		Oui		
Services de requête NetQoS Reporter/Analyzer Agissent comme des interfaces pour les rapports personnalisés et les analyses.	Oui		Oui		

Service	Autonome	Harvester	Console	DSA	Anomaly Detector
Service de rapport de NetQoS ReporterAnalyzer Exécute les rapports personnalisés, les analyses, les examens des flux et les rapports intersites.	Oui		Oui		
Outil de surveillance de NetQoS Reporter/Analyzer Interroge les composants afin de connaître les informations relatives au statut et, le cas échéant, de générer des avertissements destinés aux administrateurs. Cet outil se charge également d'exécuter des contrôles simples d'intégrité de la base de données.	Oui		Oui		

Journaux de services

Les journaux de services sont décrits dans le tableau ci-dessous : La partie initiale de chaque chemin correspond au chemin d'installation de CA Network Flow Analysis, comme les emplacements par défaut : C:\CA\NFA sur un serveur Windows ou /opt/CA/NFA sur un serveur de Harvester Linux. Le tableau répertorie également les noms et les emplacements des fichiers journaux de services sur les serveurs Windows et Linux, ainsi que tous les fichiers de configuration disponibles pour contrôler la configuration du niveau de journalisation.

informations des services/journaux	Autonome	Harvester	Console	DSA
Services Web de collecte et d'interrogation de CA NFA (Linux : nfa_collpollws) Journal : \Netflow\Logs\collpollws-wrapper.log	Oui	Oui		
Conservation de données CA NFA (Linux : nfa_dataretention) Journal : \Netflow\Logs\dataretention-wrapper.log	Oui	Oui		Oui
Proxys DNS/SNMP CA NFA (Linux : nfa_proxies) Journal : \Netflow\Logs\proxies-wrapper.log	Oui	Oui	Oui (A 2 niveaux)	Oui
CA NFA DSALoader Journal : \Netflow\Logs\dsaLoaderErrors-<aaaa-mm-jj>.log				Oui
Serveur de fichiers CA NFA (Linux : nfa_filewebservice) Journal : \Netflow\Logs\fileserver-wrapper.log	Oui	Oui	Oui (3 niveaux)	
Harvester CA NFA (Linux : nfa_harvester) Journal : \Netflow\Logs\harvester-wrapper.log	Oui	Oui		
Service de suivi CA NFA Journal : Logs\ADLog<aaaa-mm-jj>.log	Oui			

informations des services/journaux	Autonome	Harvester	Console	DSA
Interrogateur CA NFA (Linux : nfa_poller) Journal : \Netflow\Logs\poller-wrapper.log	Oui	Oui		
Service de pompage CA NFA Journal : \Netflow\logs\pumpservice-wrapper.log				Oui
Reaper CA NFA (Linux : nfa_reaper) Journal : \Netflow\Logs\RealtimeReaperErrors<aaaa-mm-jj>.log		Oui		
Source de la base d'informations de génération de rapports de CA NFA Journal : \Reporter\RIB\NFA\webapps\NFARS\WEB-INF\logs\ application.log	Oui		Oui	
Authentification unique CA Performance Center Journaux : \Portal\SSO\logs\SSOService.log \Portal\SSO\logs\wrapper.log	Oui		Oui	
Service Web de proxy DNS Journal : \ProxyServices\Logs\DnsProxyWSLog<aaaa-mm-jj>.log Configuration du niveau de journalisation (console NFA uniquement) : \ProxyServices\Web.config <add key="LogLevel" value="6"/> Valeur par défaut : 4	Oui		Oui	
NetQoS MySql (Linux : mysql) Journal : \MySql\data\<nom_serveur>.err	Oui	Oui	Oui	Oui
NetQoS NQMySql (Linux : nfa_mysqlCSE) Journal : \Netflow\Logs\oursql_error.log		Oui	Oui (A 2 niveaux)	Oui
Service de gestionnaire de NetQoS Reporter Journal : \Reporter\Logs\Manager Service Log<aaaa-mm-jj>.log Paramètre du niveau de journalisation : \Reporter\ReporterAnalyzer.ManagerService\bin\ ReporterManagerService.exe.config <setProperties Severity="6" /> Valeur par défaut : 4	Oui		Oui	
Journaux de thread du service de gestion du générateur de rapports NetQoS dans le répertoire \Reporter\Logs\ : Service de migration : MigrationLog<aaaa-mm-jj>.log Service de synchronisation de l'interrogateur : CollectorSyncServiceLog<aaaa-mm-dd>.log Service de maintenance du système : ManagerService_MaintenanceLog<aaaa-mm-jj>.log	Oui			
Services généraux de NetQoS Reporter/Analyzer Journal : \Reporter\Logs\nqservErrors<aaaa-mm-jj>.log	Oui			

informations des services/journaux	**Autonome**	**Harvester**	**Console**	**DSA**
Service de pompage de NetQoS Reporter/Analyzer Journal : \Reporter\Logs\PumpLog<aaaa-mm-jj>.log Configuration du niveau de journalisation : \Reporter\NetQoS.ReporterAnalyzer.PumpService\ bin\NetQoS.ReporterAnalyzer.PumpService.exe.config <setProperties Severity="6" /> Valeur par défaut : 4	Oui			
Services de requête NetQoS Reporter/Analyzer (services de génération de rapports) Journal : \Reporter\Logs\nqreporterErrors<aaaa-mm-jj>.log Journal de tâche de groupes automatiques : \Reporter\Logs\ManagerService_AutomaticGroupsLog <aaaa-mm-jj>.log Journal de tâche DNS : \Reporter\Logs\ManagerService_DnsLog<aaaa-mm-jj>.log Journal de tâches de maintenance : \Reporter\Logs\ManagerService_MaintenanceLog <aaaa-mm-jj>.log	Oui			
Service de rapport de NetQoS Reporter/Analyzer Journal (journal d'examen des flux) : \Reporter\Logs\ReportServiceLog<aaaa-mm-jj>.log Configuration du niveau de journalisation : \Reporter\NetQoS.ReporterAnalyzer.ReportService\ bin\NetQoS.ReporterAnalyzer.ReportService.exe.config <setProperties Severity="6" /> Valeur par défaut : 4 Pour journaliser chaque interrogation en plus de la journalisation d'événement standard : <add key="VerboseLogging" value="True"/>	Oui			
Outil de surveillance de NetQoS Reporter/Analyzer Journal : \Reporter\Logs\WatchdogLog<aaaa-mm-jj>.log Configuration du niveau de journalisation : \Reporter\ NetQoS.ReporterAnalyzer.WatchdogService\bin\ WatchdogService.exe.config <setProperties Severity="6" /> Valeur par défaut : 4	Oui			
Plusieurs processus Journal : \Reporter\Logs\ConsoleErrorsLog<aaaa-mm-jj>.log	Oui			
Journal du service Web de proxy ProductSyncWS : \Reporter\Logs\ProductSyncWSLog<aaaa-mm-jj>.log	Oui		Oui	

Procédure de sauvegarde et de restauration des données

Effectuez les opérations décrites dans cette section pour sauvegarder et restaurer les bases de données de CA Network Flow Analysis. Vous pouvez sauvegarder des bases de données CA Network Flow Analysis manuellement (suivez les instructions incluses dans cette section) ou sauvegarder les bases de données automatiquement. Pour sauvegarder les bases de données automatiquement, ajoutez les répertoires appropriés à votre routine de sauvegarde régulière, par exemple :

- Fichiers de configuration personnalisés : emplacements personnalisés (tout serveur)
- Base de données personnalisée de conservation des données : <chemin_installation>\MySql\data\data_retention (serveur autonome ou de Harvester)
- Données de présentation de l'entreprise et données de configuration de la console NFA : <chemin_installation>\MySql\data\reporter (serveur de console NFA)
- Données historiques (15 minutes) sur un serveur autonome ou dans un déploiement distribué à deux niveaux : <chemin_installation>\Netflow\datafiles\ReaperArchive15 (serveur autonome ou de Harvester)
- Données historiques (15 minutes) sur un déploiement distribué à trois niveaux : <chemin_installation>\MySql\data\nqrptr (serveur de DSA)
- Données de configuration du Harvester : <chemin_installation>\mysql\data\harvester (serveur autonome ou de Harvester)
- Données d'interrogateur : <chemin_installation>\mysql\data\poller (serveur autonome ou de Harvester)

Important :

- Vous devez exécuter les sauvegardes simultanément. Des problèmes peuvent en résulter si vous restaurez des données à partir de sauvegardes dont les horodatages sont différents. Vérifiez que vos fichiers de données sauvegardés indiquent la même heure.
- Stockez les sauvegardes à un emplacement distant pour pouvoir les récupérer en cas de panne de matériel ou de système d'exploitation sur le serveur principal. Par exemple, sauvegardez les bases de données sur un partage administratif ou un lecteur réseau mappé.

Tenez compte des remarques générales relatives à la fréquence de sauvegarde (page 180).

Avant de sauvegarder des bases de données volumineuses, tenez compte de la quantité d'espace disque requis pour les sauvegardes et de la durée de vie des fichiers que vous sauvegardez. Les données de flux brutes (fichiers NFA) ou le répertoire de fichiers de données complet ne doivent pas être nécessairement être inclus dans la sauvegarde.

Bases de données à sauvegarder

CA Network Flow Analysis utilise plusieurs bases de données pour stocker des données de configuration, des données de résolution en 15 minutes (historiques), des données de résolution élevée (1 minute) et des données de présentation de l'entreprise. Cette rubrique décrit les bases de données à inclure dans les sauvegardes et fournit des recommandations générales relatives à la fréquence de sauvegarde. Les données sont utilisées différemment dans des environnements différents, c'est pourquoi vos priorités de sauvegarde pour prévenir la perte de données peuvent varier.

All Servers (Tous les serveurs)

- Fichiers de configuration personnalisés : sauvegardez les autres fichiers de configuration personnalisés (fichiers personnalisés par vous ou par le service de support de CA).

  Emplacement : fichiers .config, .conf ou .ini localisés n'importe où à l'emplacement d'installation de CA Network Flow Analysis

  Recommandation : sauvegarde quotidienne

Programme d'authentification unique

(Déploiements de CA PC) Sauvegardez tous les paramètres de configuration d'authentification unique personnalisés sur le serveur d'authentification unique, qui peut être le serveur Performance Center. Si vous perdez des paramètres d'authentification unique personnalisés, vous risquez de ne plus pouvoir vous connecter.

- Fichiers de configuration d'authentification unique, décrits dans la rubrique Fichiers de configuration d'authentification unique du *Manuel d'installation de CA Performance Center*.

Console NFA (déploiement distribué)

- Base de données du Reporter : le contenu inclut les 24 dernières heures de données de présentation de l'entreprise, les paramètres et les informations de synchronisation.

  Emplacement : <chemin_installation>\mysql\data\reporter

  Recommandation : sauvegarde hebdomadaire

Harvester (déploiement distribué)

- Données historiques (15 minutes) (base de données ReaperArchive15 dans un déploiement distribué à deux niveaux) : le contenu de cette base de données inclut les données de résolution en 15 minutes stockées pour les routeurs de génération de rapports et les interfaces.

  Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive15

  Recommandation : sauvegarde hebdomadaire

- Fichiers de configuration du Harvester et de l'interrogateur : les données de configuration de l'interrogateur et du Harvester sont essentielles pour effectuer le mappage relationnel qui fournit l'accès aux données de résolution en 15 minutes. Les données de configuration de l'interrogateur fournissent des informations concernant les unités et les interfaces pour activer l'interrogation, telles que les ID persistants pour les interfaces.

  Emplacements : <chemin_installation>\MySql\data\harvester et <chemin_installation>\MySql\data\poller

  Recommandation : sauvegarde quotidienne

- (Facultatif) Données d'examen des flux (base de données HarvesterArchive) :

  Emplacement : <chemin_installation>\Netflow\datafiles\HarvesterArchive

  De nombreux administrateurs ne sauvegardent pas les données d'examen des flux, car leur durée de stockage est courte (maximum de 24 heures).

- (Facultatif) Fichiers de données à haute résolution (1 minute) (base de données ReaperArchive) : de nombreux administrateurs ne sauvegardent pas les données de résolution en 1 minute, car leur volume élevé requiert de longues sauvegardes. Lorsque vous décidez de sauvegarder ces fichiers, tenez compte des facteurs :

  - Valeur de ces données calculée sur une base quotidienne
  - Durée de sauvegarde élevée

  Les données de résolution en 1 minute sont stockées pendant un mois.

  Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive

- Fichiers de configuration de conservation des données personnalisées : si vous avez personnalisé des paramètres de conservation de données, sauvegardez les données de configuration de conservation de données.

  Remarque : Les paramètres de conservation de données ne sont généralement pas personnalisés, sauf avec l'aide du support CA. Les modifications apportées aux paramètres de conservation des données peuvent créer des problèmes, lorsque l'espace du lecteur utilisé augmente.

  Emplacement : <chemin_installation>\MySql\data\data_retention

  Recommandation : sauvegarde quotidienne

DSA (déploiement distribué à trois niveaux)

- Données historiques (15 minutes) (base de données ReaperArchive15 dans un déploiement distribué à trois niveaux) : le contenu de cette base de données inclut les données de résolution en 15 minutes stockées pour les routeurs de génération de rapports et les interfaces.

  Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive15

  Recommandation : sauvegarde hebdomadaire

- Données historiques (15 minutes) (base de données MySQL nqrptr) : ce répertoire contient les paramètres de DSA.

  Emplacement : <chemin_installation>\MySql\data\nqrptr

  Recommandation : sauvegarde hebdomadaire

Stand-Alone Server (Serveur JDBC)

- Base de données du Reporter : le contenu de cette base de données inclut les données de présentation de l'entreprise, les paramètres et les informations de synchronisation pour les 24 dernières heures.

  Emplacement : <chemin_installation>\mysql\data\reporter

  Recommandation : sauvegarde hebdomadaire

- Données historiques (15 minutes) (base de données ReaperArchive15) : le contenu de cette base de données inclut les données de résolution en 15 minutes stockées pour les routeurs de génération de rapports et les interfaces.

  Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive15

  Recommandation : sauvegarde hebdomadaire

- Fichiers de configuration du Harvester et de l'interrogateur : les données de configuration de l'interrogateur et du Harvester sont essentielles pour effectuer le mappage relationnel qui fournit l'accès aux données de résolution en 15 minutes. Les données de configuration de l'interrogateur fournissent des informations concernant les unités et les interfaces pour activer l'interrogation, telles que les ID persistants pour les interfaces.

  Emplacements : <chemin_installation>\MySql\data\harvester et <chemin_installation>\MySql\data\poller

  Recommandation : sauvegarde quotidienne

- (Facultatif) Données d'examen des flux (base de données HarvesterArchive) :

  Emplacement : <chemin_installation>\Netflow\datafiles\HarvesterArchive

  De nombreux administrateurs ne sauvegardent pas les données d'examen des flux, car leur durée de stockage est courte (maximum de 24 heures par défaut).

- (Facultatif) Fichiers de données à haute résolution (1 minute) (base de données ReaperArchive) : de nombreux administrateurs ne sauvegardent pas les données de résolution en 1 minute, car leur volume élevé requiert de longues sauvegardes. Lorsque vous décidez de sauvegarder ces fichiers, tenez compte des facteurs :

  - Valeur de ces données calculée sur une base quotidienne
  - Durée de sauvegarde élevée

  Les données de résolution en 1 minute sont stockées par défaut pendant un mois.

  Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive

- Fichiers de configuration de conservation des données personnalisées : si vous avez personnalisé des paramètres de conservation de données, sauvegardez les données de configuration de conservation de données.

  Remarque : Les paramètres de conservation de données ne sont généralement pas personnalisés, sauf avec l'aide du support CA. Les modifications apportées aux paramètres de conservation des données peuvent créer des problèmes, lorsque l'espace du lecteur utilisé augmente.

  Emplacement : <chemin_installation>\MySql\data\data_retention

  Recommandation : sauvegarde quotidienne

Arrêt des services

Pour préparer la sauvegarde de bases de données, arrêtez les services sur tous les serveurs Windows dans le déploiement de CA Network Flow Analysis.

Procédez comme suit :

1. Ouvrez la fenêtre Services : cliquez sur Démarrer, Panneau de configuration, Outils d'administration, Services.
2. Arrêtez le service de Harvester (service de Harvester NetQoS ou Harvester CA NFA) sur chaque serveur.
3. Patientez 15 minutes jusqu'à la fin du traitement des fichier de données.
4. Arrêtez les services CA Network Flow Analysis sur chaque serveur :

Service	Autonome	Harvester	Console	DSA
Services Web de collecte et d'interrogation de CA NFA (Linux : nfa_collpollws)	Oui	Oui		
Conservation de données CA NFA (Linux : nfa_dataretention)	Oui	Oui		Oui
Proxys DNS/SNMP CA NFA (Linux : nfa_proxies)	Oui	Oui	Oui	Oui
CA NFA DSALoader				Oui
Serveur de fichiers CA NFA (Linux : nfa_filewebservice)	Oui	Oui	Oui (3 niveaux)	
Harvester CA NFA (Linux : nfa_harvester)	Oui	Oui		
Interrogateur CA NFA (Linux : nfa_poller)	Oui	Oui		
Service de pompage CA NFA				Oui
Reaper CA NFA (Linux : nfa_reaper)		Oui		

Service	**Autonome**	**Harvester**	**Console**	**DSA**
Source de la base d'informations de génération de rapports de CA NFA	Oui		Oui	
NetQoS MySql (Linux : mysql)	Oui	Oui	Oui	Oui
NetQoS NQMySql (Linux : nfa_mysqlCSE)	Oui	Oui	Oui	Oui
Service de gestionnaire de NetQoS Reporter	Oui		Oui	
Services généraux de NetQoS Reporter/Analyzer	Oui		Oui	
Service de pompage de NetQoS Reporter/Analyzer	Oui		Oui	
Services de requête NetQoS Reporter/Analyzer	Oui		Oui	
Service de rapport de NetQoS Reporter/Analyzer	Oui		Oui	
Outil de surveillance de NetQoS Reporter/Analyzer	Oui		Oui	

Les services et la collecte de données s'arrêtent. Les fichiers de données sont traités en 15 minutes.

5. Vérifiez le répertoire suivant sur le serveur de la console NFA :

   <chemin_installation>\Netflow\datafiles\HarvesterWork

   Si le répertoire HarvesterWork est vide, sauvegardez les bases de données (page 185).

Sauvegarde des bases de données

Avant d'effectuer des sauvegardes, arrêtez les services sur les serveurs de composant CA Network Flow Analysis et vérifiez que les répertoires HarvesterWork sont vides.

Important :

- Vous devez exécuter les sauvegardes simultanément. Des problèmes peuvent en résulter si vous restaurez des données à partir de sauvegardes dont les horodatages sont différents. Vérifiez que vos fichiers de données sauvegardés indiquent la même heure.
- Stockez les sauvegardes à un emplacement distant pour pouvoir les récupérer en cas de panne de matériel ou de système d'exploitation sur le serveur principal. Par exemple, sauvegardez les bases de données sur un partage administratif ou un lecteur réseau mappé.

Procédez comme suit :

1. Identifiez les bases de données CA Network Flow Analysis et les fichiers à sauvegarder.

   Les bases de données et les fichiers à sauvegarder au niveau de CA Network Flow Analysis sont répertoriés dans le tableau ci-dessous et décrits dans la rubrique Bases de données à sauvegarder (page 180).

Base de données	Stand-Alone Server (Serveur JDBC)	Serveurs de Harvester (distribués)	Serveur de console NFA (distribué)	DSA (distribué à 3 niveaux)
reporter	Important		Important	
harvester	Important	Important		
poller	Important	Important		
ReaperArchive15	Recommandé	Recommandé		Recommandé
Fichiers personnalisés	Important	Important	Important	Important
data_retention personnalisée	Important si personnalisé	Important si personnalisé		Important si personnalisé
HarvesterArchive	Facultatif, rarement sauvegardé	Facultatif, rarement sauvegardé		
ReaperArchive	Facultatif, rarement sauvegardé	Facultatif, rarement sauvegardé		
nqrptr				Important

2. Copiez chaque fichier ou répertoire cible dans un emplacement distant.

   La liste suivante indique les emplacements de bases de données :

   - Fichiers de configuration personnalisés : divers emplacements
   - Base de données personnalisée de conservation de données : <chemin_installation>\MySql\data\data_retention
   - Base de données harvester : <chemin_installation>\MySql\data\harvester
   - Base de données HarvesterArchive : <chemin_installation>\Netflow\datafiles\HarvesterArchive
   - Base de données nqrptr : <chemin_installation>\MySql\data\nqrptr
   - Base de données poller : <chemin_installation>\MySql\data\poller
   - Base de données ReaperArchive : <chemin_installation>\Netflow\datafiles\ReaperArchive
   - Base de données ReaperArchive15 : <chemin_installation>\Netflow\datafiles\ReaperArchive15
   - Base de données reporter : <chemin_installation>\MySql\data\reporter
   - Fichiers de configuration de l'authentification unique : sauvegardez les fichiers et les répertoires ci-dessous sur le serveur d'authentification unique (il peut s'agir du serveur Performance Center).
     - Fichier <chemin_installation>\Portal\SSO\start.ini
     - Répertoire <chemin_installation>\Portal\SSO\etc
     - Fichier <chemin_installation>\Portal\SSO\conf\wrapper.conf
     - Répertoire <chemin_installation>\Portal\SSO\webapps\sso\configuration

3. Redémarrez le service NetQoS MySql et les services CA Network Flow Analysis dépendants :

   a. Dans la fenêtre Services, cliquez avec le bouton droit de la souris sur le service NetQoS MySql, puis cliquez sur Redémarrer.
   Le message de confirmation Restart Other Services (Redémarrer d'autres services) s'ouvre et répertorie tous les services CA Network Flow Analysis dépendants qui redémarreront également.

   b. Cliquez sur Yes (Oui).

   c. Le message de confirmation se ferme et les services s'arrêtent et redémarrent.

4. Redémarrez les services (page 183) de CA Network Flow Analysis.

Restauration des bases de données

Vous pouvez restaurer les données à partir d'une sauvegarde de base de données CA Network Flow Analysis. La procédure décrite dans cette rubrique a pour but de restaurer les données sur un serveur Windows, mais le chemin d'accès à la base de données est le même pour un serveur Linux.

Procédez comme suit :

1. Connectez-vous avec des droits d'administrateur.
2. Arrêtez les services de CA Network Flow Analysis (page 183).
3. Restaurez chaque fichier ou répertoire cible depuis son emplacement distant vers son emplacement d'origine :
    - Fichiers de configuration personnalisés : divers emplacements (tout serveur)
    - Base de données personnalisée de conservation des données : <chemin_installation>\MySql\data\data_retention (serveur autonome ou de Harvester)
    - Base de données harvester : <chemin_installation>\MySql\data\harvester (serveur autonome ou de Harvester)
    - Base de données nqrptr : <chemin_installation>\MySql\data\nqrptr (serveur de DSA)
    - Base de données poller : <chemin_installation>\MySql\data\poller (serveur autonome ou de Harvester)
    - Base de données HarvesterArchive : <chemin_installation>\Netflow\datafiles\HarvesterArchive (serveur autonome ou de Harvester)

- Base de données ReaperArchive : <chemin_installation>\Netflow\datafiles\ReaperArchive (serveur autonome ou de Harvester)
- Base de données ReaperArchive15 : <chemin_installation>\Netflow\datafiles\ReaperArchive15 (serveur autonome ou de Harvester)
- Base de données reporter : <chemin_installation>\MySql\data\reporter (serveur autonome, de console NFA ou de DSA)

1. Redémarrez les services CA Network Flow Analysis qui sont répertoriés dans la rubrique Arrêt des services (page 183).

Recommandations liées à la préservation de l'intégrité des données

Pour garantir l'intégrité des données et empêcher l'endommagement des bases de données CA Network Flow Analysis, implémentez les recommandations suivantes sur les serveurs ou les systèmes matériels utilisés pour l'exécution des composants CA Network Flow Analysis :

- Excluez les répertoires suivants des analyses antivirus en temps réel : C:\Windows\Temp et <chemin_installation> et tous les sous-répertoires.
- N'implémentez pas la compression de l'espace disque.
- N'installez aucun logiciel tiers, sauf les types de logiciel suivants : antivirus, gestionnaire de système et synchronisateur horaire.
- Installez les mises à jours critiques de Microsoft. Utilisez votre meilleur jugement pour décider d'installer des mises à jour facultatives.
- Défragmentez l'unité de disque le moins souvent possible. Une défragmentation fréquente n'est pas nécessaire ; les composants CA Network Flow Analysis écrivent généralement de façon séquentielle dans les bases de données et la fragmentation de données en est ainsi réduite.

Collecte de données

CA Network Flow Analysis prend en charge deux types d'architectures de déploiement :

- Déploiements autonomes et distribués d'architecture à deux niveaux
- Déploiements distribués d'architecture à trois niveaux

Dans les deux cas, les composants de produit fonctionnent conjointement pour la collecte, le traitement et le stockage des données de flux, ainsi que pour l'affichage des données dans des rapports et la génération d'interruptions, d'événements et de rapports planifiés.

Architecture à deux niveaux

Un déploiement de type architecture à deux niveaux requiert la console NFA et un ou plusieurs nouveaux Harvesters. Les nouveaux Harvesters gèrent les tâches traditionnelles du Harvester et les tâches qu'un DSA effectue dans un déploiement à trois niveaux.

L'empreinte du déploiement est réduite et le nombre de types de composants requérant une mise à niveau et une maintenance est réduit. Par ailleurs, la gestion des données requiert moins d'étapes et une fréquence réduite d'envoi des fichiers.

Les déploiements autonomes utilisent toujours l'architecture à deux niveaux : le serveur autonome héberge la console NFA et le logiciel du nouvel Harvester.

Architecture à trois niveaux

Le déploiement d'une architecture à trois niveaux comprend la console NFA, un ou plusieurs Harvesters et un ou plusieurs DSA.

Vous pouvez opter pour l'architecture à trois niveaux si la latence des serveurs de DSA est plus faible que celle des serveurs de Harvester. En outre, les serveurs de Harvester requièrent moins d'espace de stockage.

L'architecture à trois niveaux est disponible uniquement sur certains types de déploiements distribués, comme décrit dans la rubrique Versions de logiciels prises en charge pour la mise à niveau du *Manuel de mise à niveau de CA Network Flow Analysis*.

Collecte de données dans un déploiement à deux niveaux

La console NFA et le Harvester fonctionnent ensemble de la façon suivante dans un déploiement d'architecture à 2 niveaux :

Nouveau Harvester

Il extrait les flux bruts des routeurs, analyse les données et compile les données historiques (15 minutes) et les données de résolution en 1 minute. Le Harvester stocke les données suivantes :

- Données de flux bruts
- Données de résolution en 1 minute
- Données historiques (15 minutes)

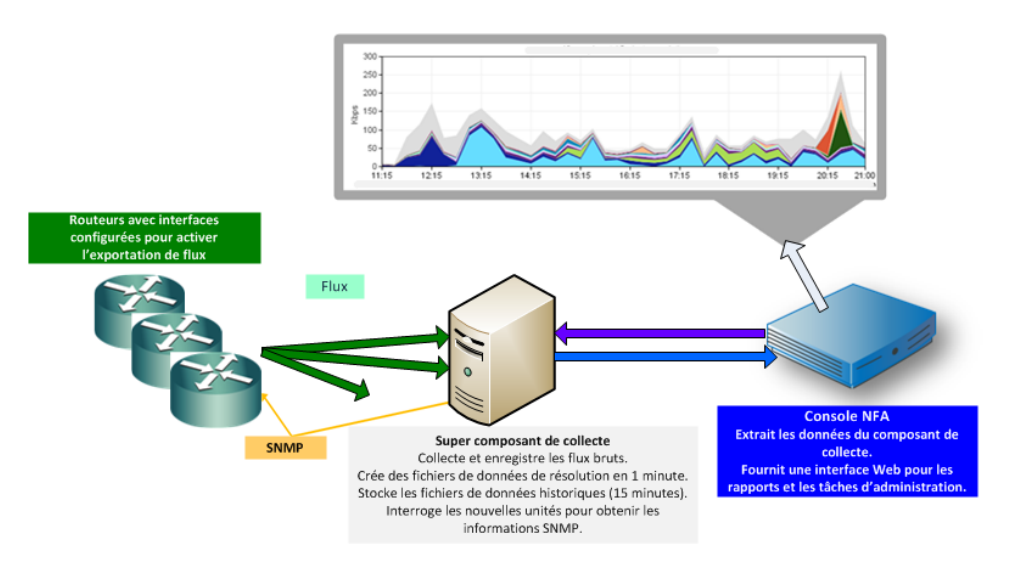
Remarque : Il est important que le serveur du Harvester dispose d'assez d'espace de stockage, car il stocke davantage de types de données que dans un déploiement d'architecture à trois niveaux.

Console NFA

Elle collecte les données à partir du Harvester et affiche les données de rapport dans l'interface Web. Elle stocke les données de présentation de l'entreprise.

Elle fournit une interface utilisateur Web pour les tâches administratives et signale et stocke les données de présentation de l'entreprise. Les rapports contiennent les données suivantes :

- Données de présentation de l'entreprise stockées localement
- Données de résolution en 1 minute et 15 minutes et données stockées sur le Harvester



Collecte de données dans un déploiement à trois niveaux

La composants de console NFA, Harvester et DSA fonctionnent ensemble de la façon suivante dans un déploiement d'architecture à trois niveaux :

Harvester

Il extrait les flux bruts des routeurs, analyse les données et les enregistre.

Il stocke les données de résolution en 1 minute données et les données de flux bruts. Les données de flux bruts des dernières 24 heures sont stockées.

Console NFA

Elle rassemble les données de présentation de l'entreprise et les données de résolution en 15 minutes (historique) à partir du Harvester et agrège les données de résolution en 15 minutes.

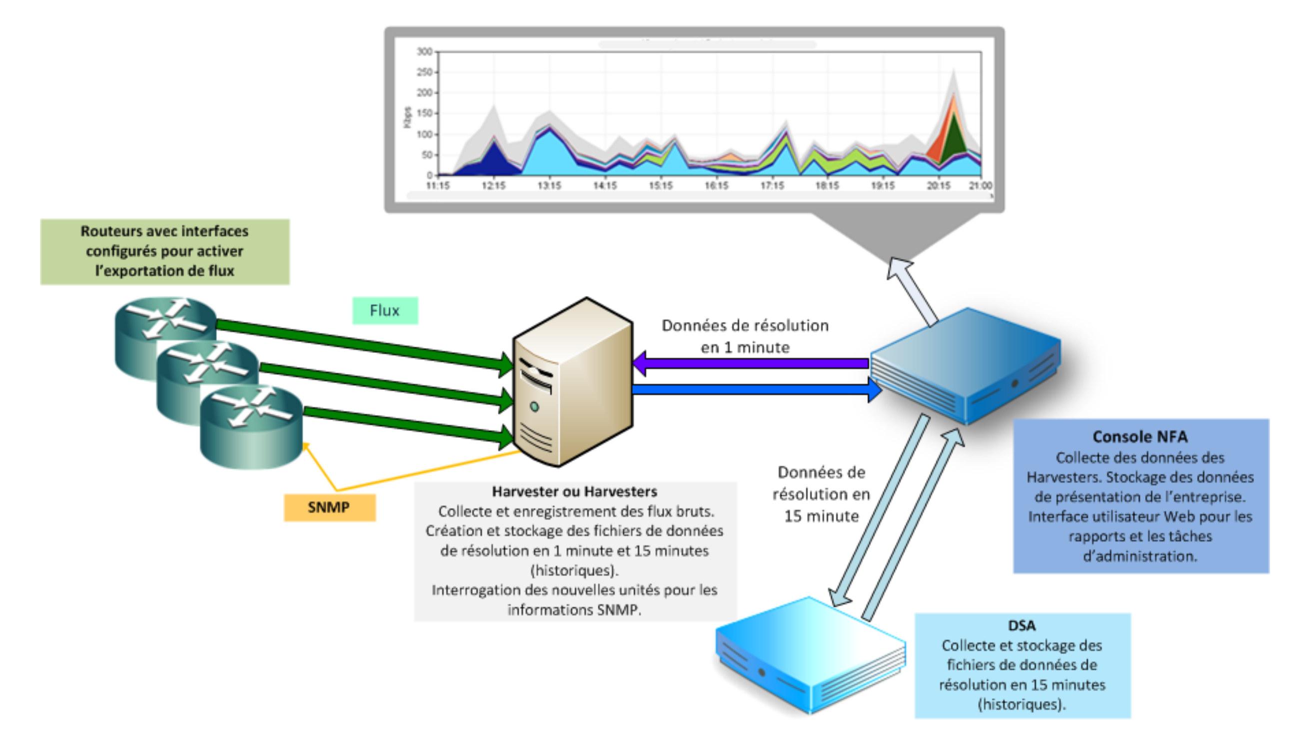
Elle stocke les données de présentation de l'entreprise.

Elle fournit une interface utilisateur Web pour les tâches d'administration et les rapports. Les rapports contiennent les données suivantes :

- Données de présentation de l'entreprise stockées localement
- Données de résolution en 1 minute stockées sur le Harvester
- Données de résolution en 15 minutes stockées sur le DSA

DSA

Il collecte les données de résolution en 15 minutes (historique) à partir de la console NFA et les stocke.



Données de la présentation de l'entreprise

Les données de présentation de l'entreprise sont collectées et affichées dans la page Présentation de l'entreprise. Pour chaque rapport, un maximum de 12 interfaces, protocoles ou hôtes est inclus pour toute l'entreprise. Les vues de présentation de l'entreprise se basent sur les 24 dernières heures de la collecte de données. Les données sont affichées dans les rapports suivants :

- Utilisation de l'interface

  Sélection : seuils définis par l'utilisateur pour l'utilisation de la capacité des interfaces.

- Principales interfaces - En entrée (trafic entrant) et Principales interfaces - En sortie (trafic sortant)

  Sélection : taux de capacité d'interface utilisée pendant la période de rapport. Le calcul de l'utilisation se base sur le volume de données et la vitesse des interfaces. La vitesse des interfaces dérive de l'interrogation SNMP.

- Principaux protocoles

  Sélectionné : volume de trafic utilisant les protocoles.

  - Principales interfaces pour le protocole

    Sélection : volume de trafic d'interfaces pour le protocole sélectionné dans la vue Principaux protocoles.

  - Principaux hôtes pour le protocole

    Sélection : volume de trafic d'hôtes pour le protocole sélectionné dans la vue Principaux protocoles.

- Principaux hôtes

  Sélection : volume de trafic total généré par les hôtes.

  - Principales interfaces pour l'hôte

    Sélection : volume de trafic d'interfaces pour l'hôte sélectionné dans la vue Principaux hôtes.

  - Principaux protocoles pour l'hôte

    Sélection : volume de trafic de protocoles pour l'hôte sélectionné dans la vue Principaux hôtes.

Durée de vie des données : les données de présentation de l'entreprise sont conservées pendant 1 mois par défaut.

Emplacement de stockage : les données sont stockées dans la console NFA dans les déploiements à deux niveaux et à trois niveaux.

Données de résolution en 15 minutes

Les types de données suivants sont collectés et stockés en tant que données de résolution en 15 minutes par défaut.

Trafic global

- Total du trafic IP, TCP et UDP entrant et sortant de chaque interface
- Flux et octets du flux de trafic entrant et sortant de chaque interface
- Total du flux de trafic de chaque routeur

Les données d'intervalle de 15 minutes reflètent les totaux pour chaque interface, mais les données de présentation de l'entreprise reflètent les totaux pour toutes les interfaces. Par exemple, les données de présentation de l'entreprise incluent les N principaux protocoles pour toutes les interfaces. Les données d'intervalle de 15 minutes incluent les N principaux protocoles pour chaque interface.

Hôtes

Le trafic sortant et entrant des 50 principaux hôtes IP

Conversations

Trafic des 50 principales conversations IP

Protocoles

- *Global :* 100 principaux protocoles entrants et sortants de chaque interface

  Les règles de places réservées vous permettent d'inclure des protocoles spécifiques dans le groupe des principaux protocoles indépendamment de leur volume de trafic.

- *Protocoles - Hôtes :* trafic sortant et entrant des 10 principaux hôtes pour les 20 principaux protocoles
- *Protocoles - Conversations :* trafic des 10 principales conversations pour les 20 principaux protocoles

Type de service

- *Global :* total du trafic IP entrant et sortant de chaque interface pour chaque valeur de type de service
- *Type de service - Protocoles :* trafic des 20 principaux protocoles pour les 5 principales valeurs de type de service non nulles
- *Type de service - Hôtes :* trafic des 10 principaux hôtes pour les 5 principales valeurs de type de service non nulles
- *Type de service - Conversations :* trafic des 10 principales conversations pour les 5 principales valeurs de type de service non nulles

Système autonome

- 100 principales sources et destinations des valeurs de système autonome
- 20 principales adresses du tronçon suivant pour chaque valeur de système autonome

Le trafic de système autonome est stocké pendant 100 jours par défaut.

Durée de vie des données : chaque type de données inclut une période de stockage maximum par défaut, comme l'illustre la liste suivante :

- Trafic global : 372 jours ou 12,4 mois
- Protocoles (100 principaux) : 372 jours ou 12,4 mois
- Hôtes, Protocoles - Hôtes et Type de service - Hôtes : 67 jours
- Conversations (50 principaux), Protocoles - Conversations et Type de service - Conversations : 67 jours
- Type de service et Type de service - Protocoles : 372 jours ou 12,4 mois
- Système autonome : 100 jours

Seuils minimum : pour être inclus dans un rapport de données de résolution en 15 minutes, le trafic de données doit correspondre aux seuils minimum par défaut ou dépasser la période de 15 minutes :

- Protocoles : 50 Ko
- Hôtes : 100 Ko
- Conversations : 100 Ko
- Type de service : Aucun minimum
- Système autonome : Aucun minimum

Emplacement de stockage : les données historiques (15 minutes) sont stockées sur le nouveau Harvester dans un déploiement à deux niveaux et sur le DSA dans un déploiement à trois niveaux.

Rapports : des tranches de données de 15 minutes sont souvent utilisées pour examiner les tendances et réaliser des analyses de capacité. Ces données s'affichent dans les rapports suivants :

- Rapports d'interface qui affichent plus de 2 heures de données
- Rapports personnalisés
- Rapports d'analyse
- Vues et rapports Performance Center qui affichent plus de 2 heures de données CA Network Flow Analysis

Données de résolution en 1 minute

Les types de données suivants sont stockés en tant que données de résolution en 1 minute par défaut.

Hôtes

Trafic sortant et entrant des 300 principaux hôtes IP

Conversations

Trafic sortant et entrant des 300 principales conversations IP

Protocoles

- *Global :* 150 principaux protocoles pour le trafic entrant et sortant de chaque interface
- *Hôtes :* trafic sortant et entrant des 25 principaux hôtes utilisant les 25 principaux protocoles
- *Conversations :* trafic des 25 principales conversations utilisant les 25 principaux protocoles

Type de service

- *Protocoles :* trafic des 25 principaux protocoles pour les 5 principales valeurs de types de services
- *Hôtes :* trafic des 25 principaux hôtes pour les 5 principales valeurs de types de services
- *Conversations :* trafic des 25 principales conversations pour les 5 principales valeurs de types de services

Durée de vie des données : la période de stockage maximum par défaut des données de résolution en 1 minute est de 1 mois.

Emplacement de stockage : les données de résolution en 1 minute sont stockées dans le Harvester dans les déploiements à deux niveaux et à trois niveaux.

Rapports : ce type de données est souvent utilisé pour le dépannage et une analyse précise. Les données s'affichent dans les rapports suivants, lorsque les rapports sont configurés pour afficher des plages horaires d'un maximum de 2 heures :

- Vues d'interface et rapports
- Vues et rapports Performance Center qui affichent moins de 2 heures de données CA Network Flow Analysis

Données brutes

Des données brutes sont utilisées pour effectuer une analyse plus détaillée au niveau des rapports d'examen des flux. Les données brutes sont stockées sur le Harvester pour un maximum de 24 heures par défaut.

Glossaire

15 minutes, données d'historique

Les données d'intervalle de 15 minutes (historique) sont des informations qui sont collectées pour chaque interface sur une plus longue période. Les informations incluent les protocoles, les hôtes et les conversations pour chaque interface. Les données récapitulatives sont également collectées pour le type de service, les principaux protocoles pour les principales valeurs de type de service et les principaux hôtes et conversations pour les principales valeurs de type de service. Les données sont stockées dans une base de données MySQL nommée nqrptr, située à l'emplacement <chemin_installation>\MySql\data\nqrptr.

Administrateur

Un *administrateur,* dans le contexte de ce document, est une personne qui est responsable de l'administration du produit dans la console NFA. Les administrateurs sont également chargés de la gestion des éléments présents dans la console Performance Center qui sont associés à CA Network Flow Analysis : profils SNMP, groupes, utilisateurs, rôles, etc.

Authentification unique

L'*authentification unique* est le schéma d'authentification qui permet aux utilisateurs de ne devoir s'authentifier qu'une seule fois pour accéder à la suite de produits associés. Une fois authentifiés, les utilisateurs peuvent passer d'un produit à l'autre sans devoir se reconnecter à chaque fois.

Base d'informations de génération de rapports (RIB)

La *base d'informations de génération de rapports (RIB)* est un système de services Web et de fichiers XML qui décrivent et fournissent les données utilisées dans les vues et tableaux de bord de la console CA Performance Center. Ces données proviennent de sources de données telles que CA Network Flow Analysis. RIB fournit un environnement d'exploitation pour la génération de rapports tiers, fédérés et interproduit. RIB utilise un service Web unique d'accès aux données avec des fonctionnalités semblables à SQL.

Console NFA

La *console NFA* est un composant dans un déploiement distribué de CA Network Flow Analysis qui fournit une interface utilisateur Web pour les rapports et les fonctions administratives. La console NFA crée des rapports à partir des données de présentation de l'entreprise, stockées localement, et à partir des données de résolution en 1 minute et 15 minutes récupérées d'autres composants.

Conversation

Une *conversation* est une session de trafic sous-réseau-à-sous-réseau ou utilisateur-à-utilisateur (hôte-à-hôte). La console NFA affiche les informations sur les conversations, afin de vous permettre de déterminer si une conversation cause par exemple une pointe de trafic sur une interface. Vous pouvez créer et exécuter des rapports pour identifier les principales conversations basées sur le volume.

Domaines IP

Les *domaines IP* sont des ensembles logiques de données provenant d'unités et de réseaux divers. Les domaines permettent à votre entreprise de surveiller individuellement les adresses IP et interfaces associées ou de superviser des applications qui appartiennent à des réseaux es réseaux clients distincts. Les administrateurs globaux peuvent surveiller les domaines IP à partir d'une console unique, mais les opérateurs peuvent voir uniquement les données associées aux domaines qu'ils sont autorisés à consulter. Les administrateurs créent des domaines IP personnalisés dans la console Performance Center. Ils peuvent utiliser la console NFA pour assigner des Harvesters, des routeurs, des interfaces, des interfaces virtuelles personnalisées et autres à des domaines IP.

Données d'intervalle de 1 minute (haute résolution)

Les *données d'intervalle de 1 minute (haute résolution)* sont des informations détaillées collectées à partir de chaque Harvester et fournies à la console NFA pour leur affichage dans les vues et les rapports. Les données incluent les principaux protocoles pour chaque interface, le trafic pour les principaux hôtes et conversations, les principales conversations pour les principaux protocoles et les principaux protocoles, hôtes et conversations pour les principales valeurs de type de service. Les données de résolution en 1 minute sont stockées dans une base de données du serveur de Harvester, sous <chemin_installation>\Netflow\data\archive.

Droit d'accès au produit

Un *droit d'accès au produit* est un type d'autorisation associé à un compte d'utilisateur dans Performance Center. Les droits d'accès au produit octroient un accès aux fonctionnalités de la console Performance Center, de la console NFA et de toutes les autres sources de données. Les administrateurs chargés de la gestion des comptes d'utilisateurs assignent les droits d'accès au produit dans la console Performance Center.

DSA (appliance de stockage de données)

Un *DSA (appliance de stockage de données)* est un composant dans un déploiement d'architecture à trois niveaux de CA Network Flow Analysis. Chaque DSA de résolution en 15 minutes (historique) à partir de la console NFA et les stocke. Dans un déploiement d'architecture à deux niveaux, les données de résolution en 15 minutes sont traitées et stockées sur le Harvester.

Flux

Un *flux* est un ensemble de paquets IP qui traversent un point d'observation de réseau pendant une certaine période. Dans CA Network Flow Analysis 9.3.0, le flux peut être de type NetFlow v5, v7 ou v9 ou de l'un des types suivants (conforme aux normes applicables au format NetFlow v5, v7 ou v9) : sFlow version 5, IPFIX, J-Flow, cFlow ou Huawei NetStream.

Pour que les données provenant de flux non testés apparaissent dans les rapports contenant des données (historiques) de résolution en 15 minutes, vous devez remplir les champs obligatoires suivants :

- L'un des champs suivants : 1 - IN_BYTES, 85 - IN_PERMANENT_BYTES, 231 - FW_INITIATOR_OCTETS, ou 232 - FW_RESPONDER_OCTETS
- Tous les champs suivants : 4 - PROTOCOL, 7 - L4_SRC_PORT, 8 - IPV4_SRC_ADDR, 10 - INPUT_SNMP, 11 - L4_DST_PORT, 12 - IPV4_DST_ADDR et 14 - OUTPUT_SNMP

Groupe

Un *groupe* est une collection d'éléments gérés organisés dans une arborescence. Les administrateurs globaux peuvent utiliser Performance Center pour créer des groupes personnalisés d'éléments gérés qu'un opérateur est autorisé à visualiser. Ces éléments gérés peuvent être de type applications, serveurs, réseaux, routeurs ou interfaces, par exemple.

Groupes d'autorisations

Les *groupes d'autorisations* définissent la portée des éléments gérés que chaque utilisateur ou opérateur peut surveiller. Ils peuvent créer et affecter des groupes personnalisés d'éléments correspondant au domaine de responsabilité de chaque utilisateur, comme des applications, serveurs, réseaux, routeurs et interfaces. Les administrateurs doivent assigner des groupes d'autorisations dans Performance Center pour donner aux utilisateurs accès aux groupes par défaut ou personnalisés.

Harvester

Un *Harvester* est un composant dans un déploiement distribué de CA Network Flow Analysis qui collecte des flux bruts à partir des routeurs. Dans un déploiement d'architecture à deux niveaux, le Harvester traite et stocke les données de résolution en 1 minute et 15 minutes. Dans un déploiement d'architecture à trois niveaux, le Harvester traite et stocke les données de résolution en 1 minute. La console NFA récupère et traite les données de résolution en 15 minutes.

IIS

IIS est le serveur Web intégré à l'application Microsoft Windows Server. IIS consiste en plusieurs services, notamment Simple Mail Transfer Protocol (SMTP). Dans les versions d'IIS antérieures à 5.0, IIS est une abréviation d'Internet Information Server (serveur d'informations Internet). Dans la version 5.0 et les versions ultérieures, IIS est une abréviation d'Internet Information Services (services d'informations Internet).

Interface

Une *interface* est un point de connexion, comme un port série, un relais de trame, un port Fast Ethernet, un module de transfert asynchrone ou un circuit virtuel permanent. CA Network Flow Analysis génère des rapports sur les interfaces logiques activées sur un routeur pris en charge, pour lequel les flux sont activés. La console NFA affiche les interfaces surveillées dans votre environnement.

Interface utilisateur Web

L'interface utilisateur Web de CA Network Flow Analysis s'affiche comme la console NFA et permet à un opérateur d'accéder aux vues et aux rapports CA Network Flow Analysis à partir d'un navigateur Web. Les administrateurs de CA Network Flow Analysis utilisent cette interface pour effectuer certaines fonctions d'administration.

Interface virtuelle personnalisée

Une *interface virtuelle personnalisée* est une représentation abstraite d'une interface réseau, qui correspond à un ou plusieurs sous-réseaux d'interfaces physiques réelles. Les interfaces virtuelles personnalisées peuvent vous apporter une visibilité suffisante sur le trafic réseau pour un cloud porteur. Configurez des interfaces virtuelles personnalisées pour le trafic de centre de données transféré aux sous-réseaux à travers un cloud porteur MPLS lorsque le flux est activé sur les routeurs du centre de données.

Interruption

Une *interruption* est un message qui indique qu'un seuil a été atteint ou qu'une autre condition définie par l'utilisateur s'est produite. Un agent SNMP envoie des interruptions à la console NFA ou à un système de gestion de réseau. L'agent de l'outil de surveillance définit un nombre d'interruptions pour la gestion du système et des applications.

LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole logiciel permettant de localiser des organisations, des individus et d'autres ressources, telles que des fichiers et des périphériques dans un réseau. Le protocole LDAP est basé sur un modèle client/serveur. Le client LDAP établit une connexion de protocole TCP vers un serveur LDAP, puis envoie des demandes et reçoit des réponses via cette connexion.

Ligne de tendance

Une *ligne de tendance* est une projection des performances à venir d'un élément en fonction des performances passées. CA Network Flow Analysis crée la ligne de tendance comme la meilleure ligne droite reliant les points de données de la période de référence.

Mappage d'applications

Le mappage d'applications est une technique basée sur des règles pour regrouper le trafic d'une application afin de faciliter la génération de rapports sur celle-ci. Les règles de mappage d'applications sont définies selon des facteurs qui peuvent inclure l'origine du trafic (hôte, sous-réseau et masque, et/ou port), le type de service et le protocole.

NetFlow

NetFlow est une transaction entre deux hôtes, qui utilise une paire unique de numéros de port et d'adresses IP et inclut certaines informations de trafic réseau. Vous pouvez configurer un routeur Cisco pour exporter des informations de flux en envoyant des paquets UDP qui contiennent des statistiques de flux à un ou plusieurs collecteurs, comme les Harvesters. CA Network Flow Analysis prend en charge les versions 5, 7 et 9 de NetFlow, et la version 5 de sFlow. CA Network Flow Analysis prend également en charge les flux IPFIX, J-Flow, cFlow et Huawei NetStream s'ils sont conformes aux normes de NetFlow v5, v7 ou v9.

Pare-feu

Un serveur de *pare-feu* est une passerelle entre un réseau local et un grand réseau non sécurisé, comme Internet. Un serveur de pare-feu exécute généralement un package logiciel qui inspecte les paquets entrants et sortants et décide de les laisser passer ou pas.

Performance Center

Dans cette documentation, le terme *Performance Center* fait collectivement référence à CA Performance Center et à CA NetQoS Performance Center. CA Network Flow Analysis est conçu pour être utilisé avec l'un de ces programmes. Les noms de page ou les fonctions spécifiques à une version de Performance Center peuvent être identifiés au moyen du nom complet ou de l'acronyme du programme. *CA PC* est l'acronyme de CA Performance Center et *NPC* celui de CA NetQoS Performance Center.

Période de génération de rapports

Une *période de génération de rapports* représente la période spécifiée par l'utilisateur à inclure dans un rapport CA Network Flow Analysis. Les options temporelles varient en fonction du type de rapport et peuvent être des heures, des jours, des semaines ou des mois.

Places réservées

Les *places réservées* sont une technique basée sur des règles permettant de garantir que les rapports incluent le trafic approprié, même si le volume ou le taux de trafic est faible. Les règles créent des places réservées dans des rapports pour les données qui correspondent aux ports et aux protocoles cibles.

Profils SNMP

Les *profils SNMP* sont des définitions qui contiennent les informations permettant d'utiliser SNMP de manière sécurisée pour interroger des MIB (Management Information Bases - bases d'informations de gestion) d'unité. Chaque connexion à une unité est établie à l'aide d'un profil SNMP. Les administrateurs créent des profils SNMP dans la console Performance Center, lorsque cela s'avère nécessaire. Dans un environnement CA Performance Center à clients hébergés multiples, les profils SNMP sont propres à chacun de ces clients hébergés. Dans ce type d'environnement, chaque Harvester utilise l'un des profils SNMP configurés pour son client hébergé parent.

Rapport

Un *rapport* est un affichage de données collectées, que vous affichez dans la console NFA à partir des pages Présentation d'entreprise, Interfaces, Génération de rapports personnalisés, Examen des flux et Analyse. Vous pouvez imprimer ou enregistrer les rapports au format PDF. Vous pouvez également exporter les rapports dans des fichiers CSV. Un administrateur peut configurer l'envoi par courriel de certains rapports à des intervalles planifiés.

Rapport d'analyse en profondeur

Un *rapport d'analyse en profondeur* est un rapport plus détaillé que vous pouvez afficher par simple clic sur un lien inclus dans un rapport. Vous pouvez, par exemple, ouvrir un rapport d'analyse en profondeur en cliquant sur un nom d'interface dans un rapport de la page Présentation de l'entreprise, par exemple. Les utilisateurs possédant les informations d'identification appropriées peuvent également passer des vues Performance Center aux rapports détaillés dans la console NFA.

Référence

Une *référence* est l'enregistrement d'un comportement typique, calculé à partir des comportements précédents. Les références vous aident à comparer les modifications dans le temps et à prévoir les données ou les performances futures. La comparaison des valeurs actuelles aux projections de la référence permet de déterminer si les valeurs actuelles sont habituelles. La référence dans un graphique de tendance est calculée à l'aide des données des six semaines précédant la plage de dates sélectionnée, à l'exception des points de données déjà inclus dans le graphique.

Rôle

Un *rôle* contrôle l'accès aux fonctionnalités de produit au niveau de la console NFA et de la console Performance Center. Dans un déploiement bien planifié, les rôles permettent aux utilisateurs d'accéder aux fonctionnalités dont ils ont besoin pour s'acquitter de leurs tâches. Les rôles limitent également l'accès aux fonctionnalités dont les opérateurs et administrateurs n'ont pas besoin. L'administrateur qui est chargé de la gestion des comptes d'utilisateurs assigne les rôles dans la console Performance Center.

SMTP

Le *protocole Simple Mail Transfer Protocol (SMTP)* est le protocole TCP/IP (Transfer Control Protocol/Internet Protocol) utilisé pour l'envoi et la réception de courriels sur les réseaux de données.

SNMP

Le *Simple Network Management Protocol (SNMP)* est le protocole de gestion de réseaux utilisé presque exclusivement sur les réseaux de données. Il s'agit d'une méthode de surveillance et de contrôle des périphériques réseau, mais également de gestion des configurations, de la collecte des statistiques, des performances et de la sécurité.

Sources de données

Les *sources de données* sont les produits qui fournissent des données à afficher dans la console Performance Center. Les sources de données fournissent également des données de configuration qui sont stockées dans Performance Center. CA Network Flow Analysis est conçu pour être une source de données pour Performance Center.

Synchronisation

La *synchronisation*, ou synchronisation globale, est un processus qui a lieu dans Performance Center et qui permet d'échanger différents types de données avec CA Network Flow Analysis, notamment la configuration. Par exemple, si un administrateur crée des comptes d'utilisateurs ou des profils SNMP, les données associées sont transmises à la console NFA au moyen d'une synchronisation. Les données sont automatiquement synchronisées toutes les 5 minutes. Les administrateurs peuvent également effectuer une synchronisation complète ou partielle sur demande.

système autonome

Le terme *système autonome* (AS) désigne un groupe connecté de préfixes de routage IP. Les préfixes de routage IP possèdent une stratégie de routage unique et définie de façon claire et ils sont contrôlés par un ou par plusieurs opérateurs de réseau. Des données de système autonome utiles apparaissent dans les rapports uniquement si les routeurs et les interfaces sont configurés pour les exporter.

tableaux de bord

Les *tableaux de bord* sont des pages dynamiques de génération de rapports dans la console Performance Center. Les tableaux de bord sont accessibles à partir de l'onglet Tableaux de bord (CA PC) ou Rapports (NPC). Chaque tableau de bord est une collection de vues qui présentent des données provenant de sources de données enregistrées dans une page Web unique. Vous pouvez personnaliser la disposition, les vues, l'intervalle de temps et le contexte de groupe de chaque tableau de bord.